LINKSYS®
思科系统公司子公司

第二层以太网可管理交换机

SR316 16 端口10/100 第二层以太网可管理交换机

SR324 24 端口10/100 第二层以太网可管理交换机

SR3016 16 端口 + 2miniGBIC 第二层以太网千兆位可管理交换机

SR3024 24 端口 + 2miniGBIC 第二层以太网千兆位可管理交换机



Web-based Interface

用户手册

V 1.00

CISCO SYSTEMS

目　　　录

5.5.5 生成树端口配置 38

5.5.8 GARP 配置 43

5.9.2 交换机摘要 101

5.11.6 Ping 117

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors which may appear in this guide.

Ethernet is a trademark of XEROX Corporation. Microsoft, Windows and Windows logo are trademarks of Microsoft Corporation.

The revision date for this guide is **Feb. 20th, 2004**
Version 1.0b

FCC Statement

This product has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such interference when operating in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used according to the instructions, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause interference in which case the user, at his or her own expense will be required to take whatever measures may be required to correct the interference.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

1: 介绍

本使用手册适用于下列各型千兆位以太网可管理交换机:
SR316
SR324
SR3016
SR3024

若无特别指定型号则泛指上列所有交换机.在这个使用手册全文中，可管理交换机或交换机皆指此千兆位以太网可管理交换机。

本千兆位以太网可管理交换机被设计为第二层交换机,提供了管理上统治能力和多个端口。严密地遵守网络标准，本千兆位以太网可管理交换机容易地适合您的网络布局,且能经由控制台和互联网浏览器执行它的可管理功能。

1.1 组件内容

包含以下:

- 一个千兆位以太网可管理交换机
- 一条电源线
- 安装托架
- 一串行/控制台电缆
- CD - 使用手册

任何所列项目若有是缺损，请与购买处联系。

1.2 怎么使用本手册

本使用手册的构造如下:

- 第 2 章，*安装* 说明本交换机功能及如何进行实际架设.
- 第 3 章，*配置* 说明如何设定及修改本交换机的配置.

- 第 4 章，*命令行界面控制台管理*
- 第 5 章，*基于互联网的管理* 说明如何通过互联网浏览器管理本交换机.

2: 安装

这个章节描述可管理交换机的功能和显示如何在安装桌上或架子上。读者应具备连网的基本知识,请先完全阅读了这个章节。

2.1 产品描述

2.1.1 概述

SR3xxx 系列千兆位以太网可管理交换机具有强大网络可管理功能和弹性连接组合的第二层交换机。
SR316 具有 16 个 10/100 Mbps 端口和两个可选用的千兆位 Combo 模块,SR324 具有 16 个 10/100 Mbps 端口和两个可选用的千兆位 Combo 端口。此千兆位 Combo 端口具有一个 10/100/1000 Mbps 端口和一个 miniGBIC 插槽。
SR3016 具有 16 个 10/100/1000 Mbps 端口和两个可选用 miniGBI 的插槽,SR3024 具有 24 个 10/100/1000 Mbps 端口和两个可选用 miniGBI 的插槽。
严密地遵守网络标准,本交换机能容易地适合您的网络布局及管理工作,且能经由控制台和互联网浏览器执行管理功能, 多样化的管理途径窗户和易于使用的界面,如控制台,远程登录程序,和互联网,有利于管理人的工作, 把管理的开销减至最小量。

2.1.2 SR316/SR324 的特性

- 16/24 个 10/100 自适应端口及两个可共享的千兆位 Combo 端口
- 所有的 10BASE-T/100BASE-TX/1000BASE-TX 端口皆支持半双工及全双工模式
- 所有的端口自动侦测 MDI/MDI-X 及所有的 100/1000 端口。
- 自动极性侦测和允许纠正所有 RJ-45 端口为联机错误的自动调整。
- 每一个 egress 端口支援达四个 Class of Service (CoS)队列。
- 实行两种机制,cell-based HOL blocking 及 packet-based HOL blocking, 以防止 Head Of Line Blocking 于每一个端口为基础。
- 支援一种分封 aging 机制它允许交换机放弃一个存于交换机分封存储器。此分封 aging 限制为可编程和有大约 515 秒中的最大时间持续时间。
- 支持机制以处理 backpressure 而可以弹性流量控制于分封交易,此限制基于侦测到在输入端口存储器利用的数量,此限制为可设定。
- 提供可编程临限限制以防止分封溢出到网络的其它部分. 三种类型的分封能够监控且每

一种类型分封都各有计数器。

- 支持对每一端口的入口和出口的端口镜像。
- 完全符合 IEEE 802.1D 生成树规范。
- 支持 IEEE 802.1s 规范之单一端口多生成树。
- 支持 IEEE 802.1p 规范。
- 支持 IEEE 802.1Q 规范之虚拟桥接区域性网络。
- 提供相同的速度的最多达八个端口能组成一个集群的机制，最多能建立六个集群。
- 支持包含式及不包含式过滤针对分封的协议做过滤和分类。
- 可利用 Console, Telnet, Web, SNMP/RMON 管理。

2.1.3 SR3016/SR3024 的特性

- 16/24 10BASE-T/100BASE-TX/1000BASE-TX 端口及两个共享的 Mini-GBIC 插槽。
- 所有的 10BASE-T/100BASE-TX/1000BASE-TX 端口皆支持半双工及全双工模式。
- 所有的 100/1000 绞式端口自动侦测 MDI/MDI-X。
- 自动极性侦测和允许纠正所有 RJ-45 端口为联机错误的自动调整。
- 每一个 egress 端口支援达八个 Class of Service (CoS)队列于。
- 实行两种机制,cell-based HOL blocking 及 packet-based HOL blocking，以防止 Head Of Line Blocking 于每一个端口为基础上。
- 支援一种分封老化机制它允许交换机丢弃一个存于交换机分封存储器的包。此分封老化限制为可控制
- 支持机制以处理 backpressure 而可以弹性流量控制于分封交易,此限制基于侦测到在输入端口存储器利用的数量,此限制为可编程。
  - 支持 IEEE 802.3x 流量控制全双工端口
  - 半双工端口支持干扰机制
  - IEEE 802.3z 非对称流量控制
- 提供可控制临限限制以防止分封溢出到网络的其它部分,能够监控三种类型的分封且每一种类型分封都各有计数器。
- 支持对每一端口的入口和出口的端口镜像。
- 完全符合 IEEE 802.1D 生成树规范。
- 支持 IEEE 802.1s 规范之单一端口多生成树。
- 支持 IEEE 802.1p 规范。
- 支持 IEEE 802.1Q 规范于虚拟桥接区域性网络。
  - 4,096 虚拟桥接区域性网络(VLAN) 群.
  - 独立 VLAN 学习(IVL).
- 提供相同的速度的最多达八个端口能组成一个集群的机制，最多能建立 32 个集群。

- 支持包含式及不包含式过滤针对分封的协定做过滤和分类。
- 支援长达 9-KB 巨型帧分封
- 流量定形及量测能力
- Loss-less 模式于零分封遗失应用
- 支持快速生成树
- 可利用 Console, Telnet, Web, SNMP/RMON 管理。

2.1.4 SR316/SR324 的面板

此交换机的面板在中央位置具有 16/24 个 10/100 Mbps 端口,左方为端口状态指示灯,右方为千兆位端口,如图 2-1/2-2 所示.表格 2-1 显示端口功能, 状态指示灯的功能将在 2.1.6 节说明。用于选配插槽的插入模块将在 2.1.7 节说明。

图 **2-1 SR316** 的面板

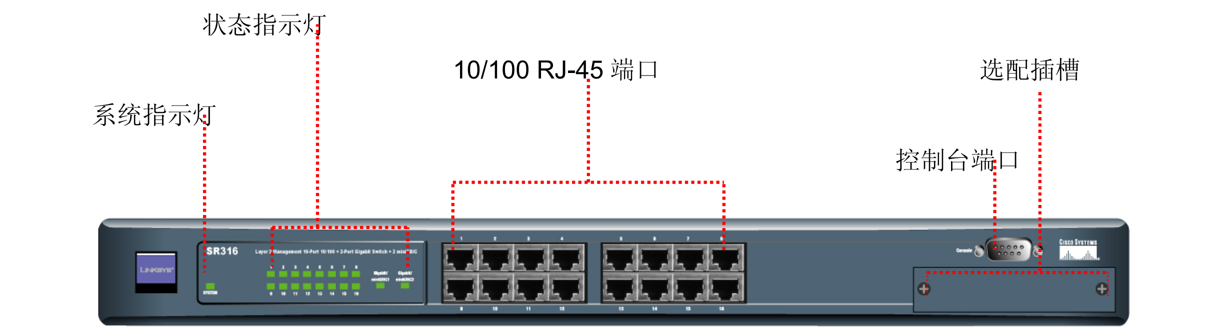


图 **2-2 SR324** 的面板

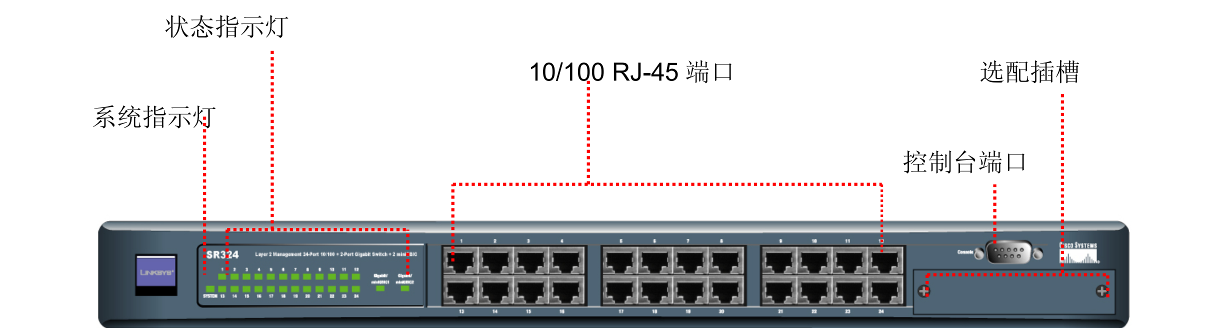


表 **2-1** 端口功能

端口	端口数量	说明
控制台	1	让你用 pc 的 RS232 端口来设定此交换机
10/100	16/24	这些 RJ-45 端口支持网络速度为 10Mbps 或 100 Mbps 可在半双工或全双工模式操作

2.1.5 SR3016/SR3024 的面板

此交换机的面板在中央位置具有 16/24 个 10/100/1000 Mbps 端口,左方为端口状态指示灯,右方为两个 miniGBIC 插槽,如图 2-3/2-4 所示.表格 2-2 显示端口功能, 状态指示灯的功能将在.2.1.6 节说明。

图 **2-3 SR3016** 的面板

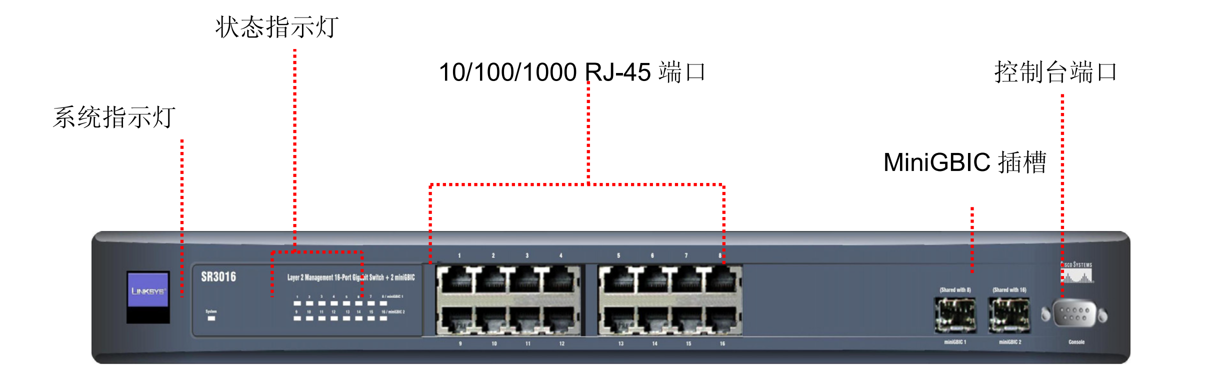


图 **2-4 SR3024** 的面板

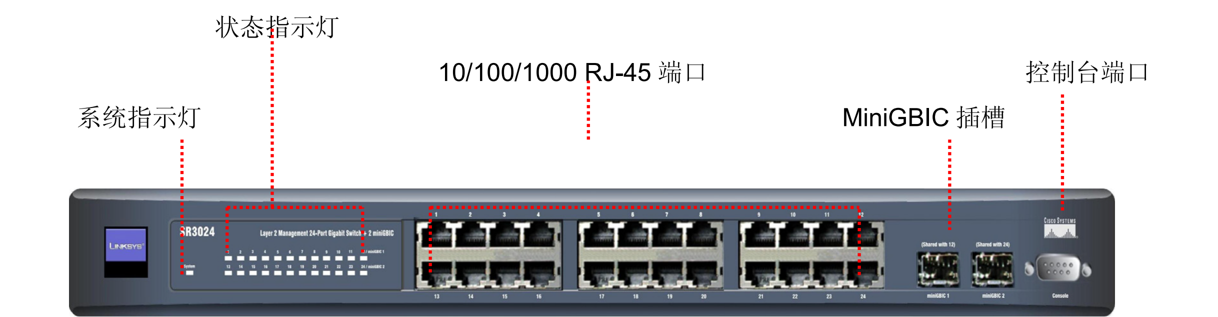


表 **2-2** 端口功能

端口	端口数量	说明
控制台	1	让你用 pc 的 RS232 端口来设定此交换机
10/100/1000	16/24	这些 RJ-45 端口支持网络速度为 10, 100 or 1000 Mbps 可在半双工或全双工模式操作
miniGIBIC	2	两个 miniGBI 的插槽用于各种光纤连接端口

2.1.6 指示灯

位于面版最左为一系统指示灯,每一端口各有一个状态指示灯,如图 2-5,2-6, 2-7,2-8 所示。表格 2-3 说明指示灯的功能。

表 **2-3** 指示灯的说明

指示灯	颜色	功能
系统	绿色	*恒亮* 表示电源正常且系统正常运作中
端口状态指示灯	绿色	*恒亮* 表示此端口已经与另一端口正常连接 *闪烁* 表示此端口正在进行数据传输中

图 **2-5** SR316 的指示灯



图 **2-6** SR324 的指示灯



图 **2-7** SR3016 的指示灯

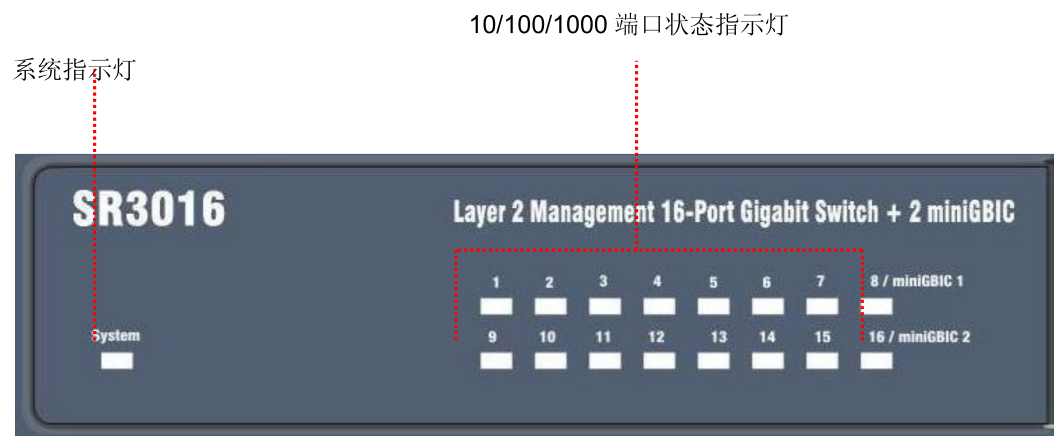


图 **2-8** SR3024 的指示灯



2.1.7 选配的插入模块

共有四种插入模块用于 SR316/SR32 交换机,如图 2-9 所示。插入模块的端口说明如下列表格。

图 **2-9** 选配的插入模块



表**2-4** 选配的插入模块

类型	端口数目	说明
100 FX	1	一个100 FX光纤端口
2-100 FX	2	两个100 FX光纤端口
Gigabit Combos	2	两个SFP端口共享GTP端口给不同的光纤接头
Gigabit Combo & 100FX	2	一个 SFP端口共享GTP端口给不同的光纤接头与一个100FX fiber 端口

2.1.8 背板

背版如图 2-10 所示有一电源插槽。

图 2-10 SR316/SR324/SR3026/SR3024 的背板



2.2 架设交换机

此交换机被设计用于办工室使用,可任意放置, 或置于桌面上,或装置于19英寸设备架上.如果你愿意可用所附的两个托座及六个螺钉将其架设在设备架上或设备间中.

在选择架设位置时,请观察下列指导方针:

- 确定交换机可以接近及电缆容易连接
- 与电气噪声来源保持距离, 如无线电,传送器, 宽频放大器及荧光灯配件
- 将交换机置于干燥之处且防止水进入
- 确保交换机四周无障碍物阻碍空气流通. 我们建议你保留最少50毫米的空间.
- 不要放置液体或其它东西于交换机上
- 如果交换机任意放置不要堆栈多于四个再任一个交换机上.

2.2.1 安装前考虑

快速以太网拓扑考虑

如果你将把这交换机以快速以太网(100Mbps)运作, 遵循下面的方针:

- 无屏蔽双绞式（UTP）五类电缆的最大长度为100米(328英尺).
- 单中继器拓扑容许网络跨度总长为325米(1066英尺).

全双工考虑

此交换机提供全双工于所有以快速以太端口. 全双工运作容许数据帧同时发送与接收以加倍

吞吐量. 如果你使用本交换机于全双工模式，五类电缆的最大长度为100米(328英尺).

2.2.2 置于桌上或安装于柜中

简单地完成以下步骤即可安装此交换机于桌上或安装于柜中:

步骤 **1** 放置交换机于接近 AC 电源处.
步骤 **2** 交换机与四周物品保持适当距离.
步骤 **3** 把这个交换机连接在网络设备上

A. 把标准的网络电缆的一个末端连接在交换机前面的 10 / 100 端口上个。
B. 把电缆的另一个末端连接在例如服务器, 工作站或路由器的网络设备上。

注: 强烈建议使用 RJ-45 接头的五类网络电缆

步骤 **4** 给交换机连接电源.

A. 电源电缆的一个末端连接在交换机.
B. 电源电缆的另一个末端连接在标准的墙上插座.

系统运作后系统指示灯应保持绿色恒亮.

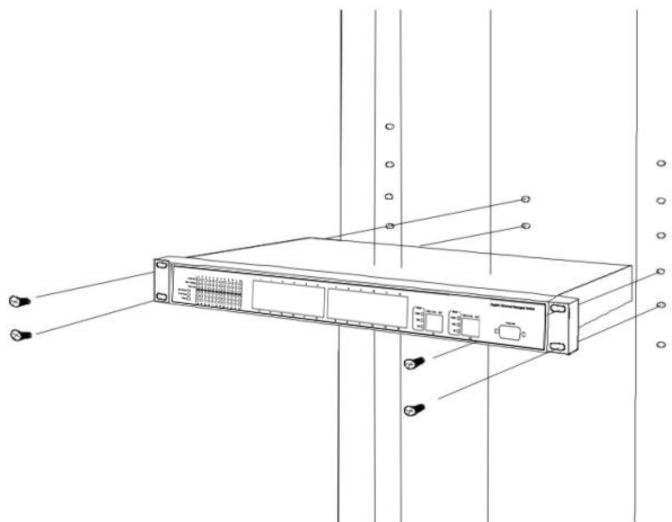
2.2.3 安装于设备架上

以下步骤说明如何将交换机安装在19英寸设备架上.

- 将交换机所有电缆移除
- 把所有胶黏衬垫从交换机的底部移除

步骤 **1** 将交换机正确朝上,前面板朝你.
步骤 **2** 托座对准交换机一边的安置孔
步骤 **3** 插入三个螺钉并用螺丝起子旋紧.
步骤 **4** 重复前两步骤于交换机的另一边
步骤 **5** 将交换机放入19英寸设备架上并适当地旋紧. 确定交换机的通气孔无阻碍.
步骤 **6** 将网络电缆与电源电缆连接到交换机.

图2-11 将交换机安装在19英寸设备架上



2.2.4 开机自我测试(POST)

当你启动交换机电源它将执行开机自我测试. 在自我测试时, 交换机的CPU:

- 执行一连串的诊断步骤以确定基本系统运作正常.
- 将交换机的主软件由快闪式存储器解压缩到动态随机存取存储器.
- 开始执行交换机的主软件B.

3:配置

这个章节说明配置管理交换机的方法。它描述管理应用系统和通信的类型和在您的管理设备(工作站或个人计算机)与系统之间提供数据的管理协议。它并且包含关于端口连接选择的信息。

这个章节包括以下题目:

- 配置管理的概要
- 关键概念
- 实施关键指南为
- 使用控制台管理
- 使用互联网管理
- 使用 SNMP 管理
- 标准、协议，和相关阅读

3.1配置管理的概要

此交换机使用以下任何或所有方法让您灵活地管理交换机:

- 管理控制台
- 浏览器界面
- 一种外在的基于 SNMP 的网络管理应用系统

管理控制台和浏览器界面支持的应用系统被嵌入在交换机的软件中，是可直接使用的。每个这些管理方法有他们自己的好处。表 3-1 比较三个管理方法。

表 3-1 三个管理方法比较

管理方法	优点	不足点:
控制台	● 没有IP地址或者subnet的需要 ● Text-based ● 安全 ● Hyper终端访问全部的功能性(Hyper终端已经构筑进了Microsoft Windows 95/98/NT/2000操作系	● 必须靠近交换机或者dial-up连接 ● 不便于远程使用 ● 非图形界面

	统	
Web浏览器或者远程登录	● 对于远程配置交换机是十分理想的 ● 熟悉的浏览器界面 ● 可利用图形似的数据 ● 最真实的要求	● 没有安全保障(计算机黑客如果知道你的IP地址的话就可以进行攻击) ● 在连接质量差的线路上可能会有延迟.
SNMP代理	● 在管理信息基础层上具有通信和交换的功能 ● 建立在开放式标准之上.	● 需要SNMP管理软件 ● 所有三个方法中在视觉上的最差 ● 一些设置需要考虑 ● 没有安全保障(黑客只需要知道团体名就可以)

3.1.1 管理控制台

管理控制台是一种以内部的,基于字符的,及命令行的用户界面为进行系统管理，譬如显示统计或改变选择设置。运用这个方法, 您能由个人计算机、苹果计算机公司的Macintosh,或工作站连接到交换机的控制台(串行)端口查看及管理交换机。
有二种方式使用这个管理方法: 经由直接电缆连接或调制解调器端口连接。以下部分描述这些方法。对于关于使用控制台的更多信息, 参见章节 4 命令行界面控制台管理。

3.1.2 直接存取

直接电缆连接对管理控制台是以直接连接终端机或具有终端仿真程序(譬如 HyperTerminal)的个人计算机到交换机控制台(串行)端口来达到目的.
要使用这个管理方法, 必需连接一个无效调制解调器在交换机与个人计算机之间。在建立这个连接以后, 配置终端仿真程序使用以下参数:

缺省参数是:

- 115,200 bps
- 8 data bits
- No parity
- 1 stop bit

如果需要改变这些设置,可在您登录之后。这个管理方法因为您能在系统重起期间保持连接和监测系统,故较为使用者喜接受。而且不管此界面相关的动作刚被启动, 某些错误信息便会寄发到此串行端口。Macintosh 或个人计算机联机可能使用任一个终端仿真程序以连接到终端串行端口。一个工作站附件在 UNIX 之下可能使用一个仿真器譬如 TIP 。

3.2 互联网管理

此交换机提供一个浏览器界面让您远程地配置和管理交换机。在设定交换机的IP地址以后,在您的浏览器输入交换机的 IP 地址而直接地能使用交换机的界面应用程序。然后从一个中央地点你可用浏览和管理交换机配置参数,好象您直接地连到交换机的控制台端口。对于更多信息,参见章节 5,浏览器管理。
互联网管理必需使用 Microsoft Internet Explorer 4.01 版本或以后版本或 Netscape Navigator 4.03 版本或以后版本。

3.3 基于 SNMP 的网络管理

您能使用一种外在基于 SNMP 程序以配置和管理此交换机。这个管理方法要求在交换机此 SNMP 代理和 SNMP 网络管理工作站使用相同群社字符串。实际上这个管理方法,使用二种群社字符串: 获取群社字符串和设定群社字符串。如果 SNMP 网络管理工作站只知道设定群社字符串,它可能给 MIBs 读和写。但是,如果它只知道得到获取群社字符串,它可能只读 MIBs 。此交换机缺省的获取和设定群社字符串为是 public。

3.4 协议

交换机支持以下协议:

- 虚拟终端协议,譬如 Telnet
- 简单网络管理协议(SNMP)

3.4.1 虚拟终端协议

一个虚拟终端协议是一个软件程序,譬如 Telnet,允许您从 Macintosh 、个人计算机,或 UNIX 工作站建立管理会话。由于 Telnet 在 TCP/IP 上执行,在建立以一个虚拟终端协议对它配置之前您必会话须有至少一个 IP 地址被配置给交换机。

注意 :Terminal 仿真与一个虚拟终端协议不同,您必须直接地连接终端到控制台(串行) 端口。

3.4.2 SNMP 协议

简单网络管理协议(SNMP) 是手多制造商 IP 网络的标准管理协议。SNMP 支持交易为基查询它允许协议将信息格式化和在报告设备与数据收集传编程间送信息。SNMP 在用户数据报协议(UDP)上层执行，提供无连接模式服务。

3.4.3 管理架构

所有管理应用程序模块使用同样应用编程界面(MAPI) 。利用简单的 MAP 将管理方法统一，以一种方法(例如控制台端口)设定参数可立即在其它管理方法(例如，浏览器的 SNMP 代理)中显示 。

此交换机的管理结构遵守 IEEE 开放标准。这种遵循给顾客保证了此交换机与其它遵守同样开放标准的设备兼容且互连。

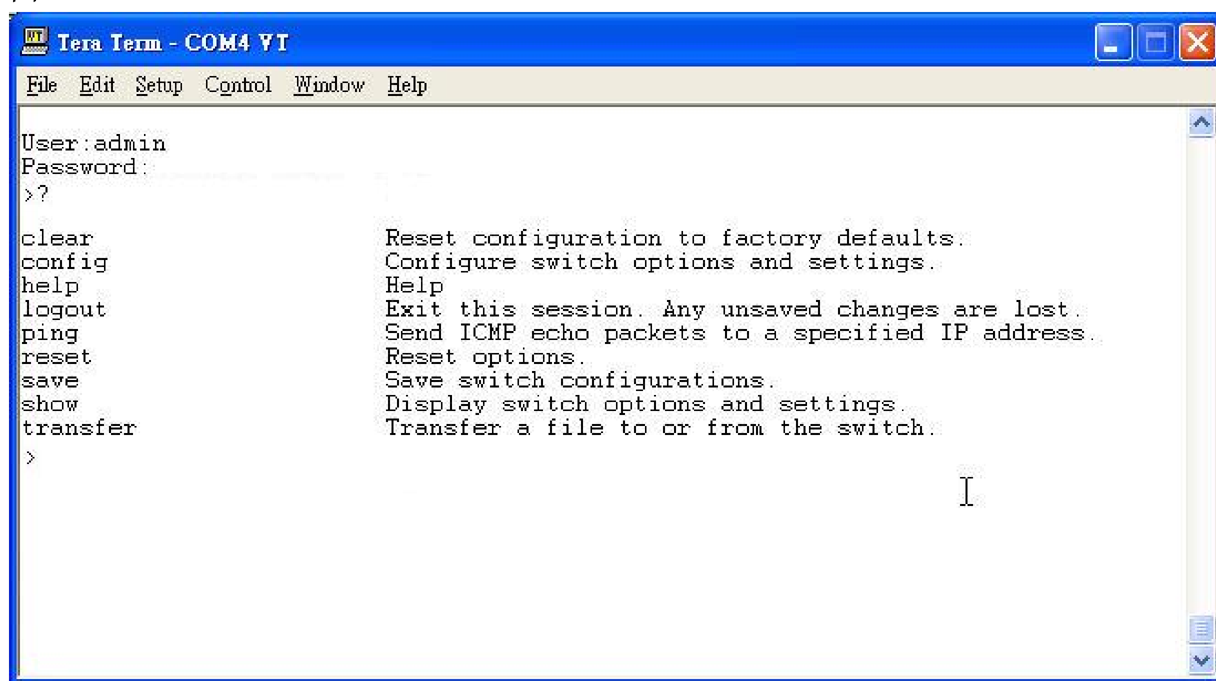
4: 命令行界面控制台管理

此交换机为配置而提供一个命令控制台界面。此交换机可经由它的 RS-232 端口(无效调制解调器模式)在当本地配置或者由远程通过 Telnet 对话配置。这个章节描述怎么使用控制台命令行界面配置交换机。

4.1 登录到交换机

登录到此交换机:
输入控制台界面工厂缺省用户名字"admin"与工厂缺省口令"" (或如果您改变了工厂缺省口令输入一个用户定义的口令) 。交换机管理屏幕在 figure 4-1 出现。

图 4-1



4.2 CLI命令

所有CLI命令请参照CLI User Guide.

5. 基于互联网浏览器的管理

此交换机提供基于互联网的浏览器界面配置和管理交换机。此界面允许你使用你的 Web 界面访问交换机。此章节描述怎么使用浏览器界面配置和管理交换机。

5.1 登录到交换机

登录到此交换机:

1. 在你的浏览器 url 栏指定交换机的 IP 地址。系统第一页将出现如图 5-1 所示画面。

图 **5-1** 系统第一页



1. 点击第一页的图标即弹出密码信息窗口，如图 5－1，输入工厂缺省用户名称 admin 或从 Login ID 下拉列表点击一个用户名称。

图 **5-2** 密码信息视窗

Password Information - Microsoft Internet Explorer

Password Input Login

Login ID : admin

Password : ●●●●●●

2. 如果你改变了工厂缺省密码，密码栏在输入用户定义的密码(或输入工厂缺省密码，工厂缺省密码是空）。
3. 点击注册按钮。交换机的系统信息在图 5-3 出现。

图 5-3 系统信息屏幕

LINKSYS® A Division of Cisco Systems, Inc.

SRxxxx Gigabit-Switch

Cisco Systems

系统信息

系统信息 | IP配置 | Switch 配置 | QoS | 安全 | 管理 | 统计表 | 纪录 | 维护 | 帮助

| 系统描述 | 系统模式 | 转发数据库 | 多播转发数据库 |

型号	SR324G2 L2 Managed Switch
系统名称	
系统位置	
系统联系者	
IP地址	172.16.0.140
系统物件ID	1.3.6.1.4.1.3955.6.4.1
系统在线时间	0 days, 1 hours, 40 minutes
基本MAC地址	00:0C:41:33:ED:1D
硬件版本	1.00
软件版本	1.000

提交

完成 我的電腦

5.2 了解浏览器界面

当你首先存取交换机浏览器界面，交换机的图标出现，与系统信息一起(参见图 5-3) 。

交换机图标提供以下标签选项为用以配置和管理交换机。

- **系统信息**---让你查看交换机的基本的信息譬如系统说明、系统方式,和转发数据库。参见章节 5.3’观察系统信息’。
- **IP配置**---让你查看交换机的IP地址和ARP表信息。参见章节5.4’观察IP配置’ 。
- **Switch配置**---让你改变端口配置、VLAN 、PVID, 链路聚集, 端口检测,GARP设置, 和IGMP侦测 设置。参见章节5.5 ’设定的交换机配置’。
- QoS---让你指定服务质量参数。在QoS 有二组命令，一组是区分服务 (DiffServ) 另一组是带宽分配(BAP) 。DiffServ的参数为包括类命令、策略命令, 和服务命令。BAP的参数包括一些命令设置流量等级。参见章节5.6 ‘执行服务质量参数’。
- **安全---**让你执行访问控制列表、802.1X访问控制设置, 和RADIUS认证。参见章节5.7’安全’。
- **管理**---让你执行用户帐号、SNMP群和trap配置设置。参见章节5.8 ’管理’。
- **统计**---让你查看交换机信息摘要、端口统计, 和链路群的信息。参见章节5.9 ’统计’。
- **记录**---让你查看交换机的系统记录。包括信息记录和事件记录。参见章节5.10’记录’。
- **维护**---让你执行交换机安装,包括网络连通性、Telnet,串行端口配置、TFTP、系统重新设置,和ping命令。参见章节5.11’维护’。
- **帮助**---当你设置你的系统有障碍时让你查看帮助信息。

每页上面是交换机的指示灯面板。指示灯面板显示各个端口的状态。你可以移动鼠标到各端口的指示灯,由下拉菜单来选择该端口的特定的信息。

5.3 观察系统信息

指向指示灯面板之下的菜单选项,点击标签’**系统信息**’,将出现以下屏幕.

图 5-4 系统信息屏幕



此屏幕显示各个端口的当前状态表。它包含以下信息:

- 系统描述－ 展示或让你配置系统的基本信息。参见章节 5.3.1 ’系统描述’。
- 系统模式－ 展示或让你配置系统的基本配置。参见章节 5.3.2 ’系统模式’。
- 转发数据库 － 让你设定 MAC 表的老化间隔及展示 MAC 表。参见章节 5.3.3 ’转发数据库’。
- 多播转发数据库 －展示多播转发数据库及让你定义多播转发的 MAC 地址。参见章节 5.3.4 ’多播转发数据库’。

5.3.1 系统描述(System Description)

图 5-5 系统信息屏幕

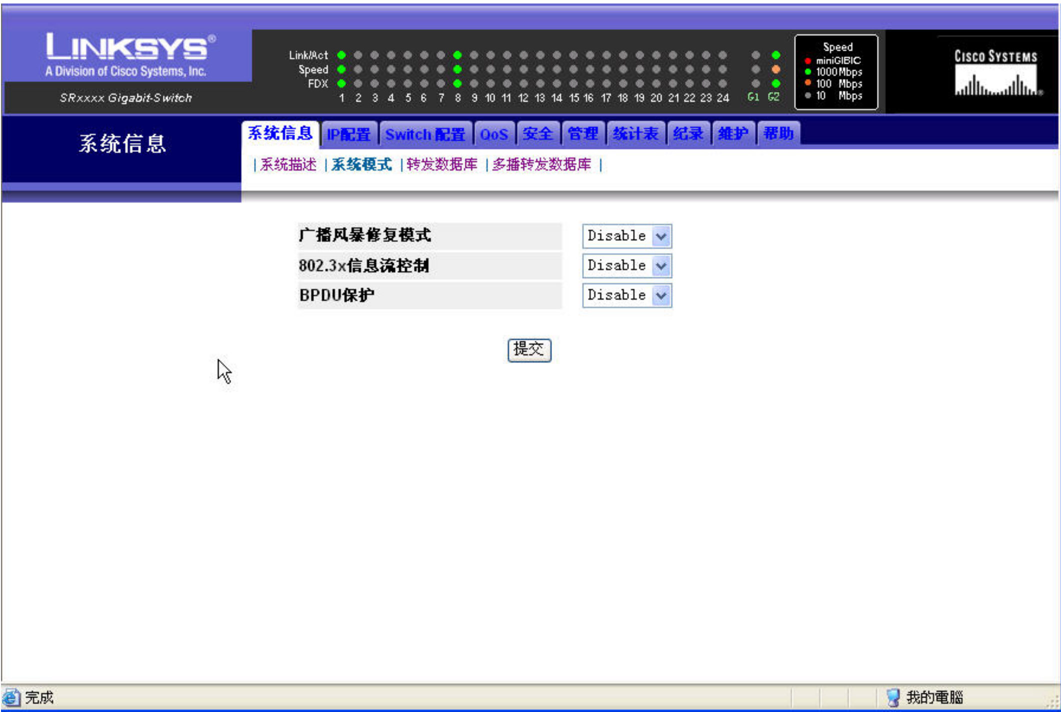


参数如下

- 型号－显示此交换机的产品型号.
- 系统名称－显示及设定此交换机的名称,一般由 31 个字母数字组成.工厂缺省值是空的.
- 系统位置－显示及设定此交换机的位置,一般由 31 个字母数字组成.工厂缺省值是空的.
- 系统联系者－显示及设定此交换机的管理人,一般由 31 个字母数字组成.工厂缺省值是空的.
- IP 地址－显示指派给交换机的 IP 地址.
- 系统对象 ID－显示此交换机的企业 MIB 的基本对象 ID.
- 系统在线时间－显示从交换机重新激活到现在的时间,以日,时和分计时.
- 基本 MAC 地址－显示此交换机的 MAC 地址.
- 硬件版本－显示此交换机的硬件版本.
- 软件版本－显示此交换机的软件版本.

5.3.2 系统模式(System Mode)

图 5－6 系统模式屏幕



广播风暴修复模式－此栏位开启或关闭广播风暴修复模式.如果是enabled, 达到高临限及低临限广播风暴修复便被施行.

临限的施行是根据一个百分比形式. 如果广播流量在任一以太网端口超过链接速度的高临限百分比(如表5-1所示)时, 此交换机丢弃这些广播流量直到广播流量回到或低于低临限百分比.完整的施行被描述在'广播风暴修复临限表'.

表 5-1 广播风暴修复临限

链接速度	高	低
10M	20	10
100M	5	2
1000M	5	2

802.3x 信息流控制---此栏位开启或关闭此交换机的802.3x信息流控制.此命令只用在全双工端口,工厂缺省值是 disabled.

BPDU保护---此栏位开启或关闭BPDU保护模式.

5.3.3 转发数据库(Forwarding Database)

图 **5-7** Forwarding Database 屏幕



- 老化间隔—此栏位配置转发数据库地址老化的时间.缺省值是 300 秒.
- 转发数据库表—此表显示所有端口的所学的信息。这些信息包括

VLAN ID –此端口的 VLAN ID, 在此处学得到那些对应事例.

MAC 地址–交换机已转发或过滤信息的 MAC 地址.格式是由冒号分开的 6 个二位十六进制数, 例如 01:23:45:67:89:AB.

端口–学到此地址的端口.

ifIndex –此端口所属的接口.

状态 – 此列项目的状态.其值意思为:

Static 此对应的事例的值由系统或用户增加,无法重学.

Learned 此对应的事例的值由学习得到,而被使用.

Management 此对应的事例的值也是dot1dStaticAddress以存在此对应的事例.当前被使用当enable VLAN做为routing时.

Self 此对应的事例的值是系统 自己的MAC.

GMRP Learned 此对应的事例的值是经由GMRP学习得到的.

Other 此对应的事例的值并非其它一类.

5.3.4 多播转发数据库(Multicast Forwarding Database)

图 **5-8** 多播转发数据库屏幕



多播转发数据库(MFDB)持有所有现行的多播地址项目与端口的成员关系信息.该项目主要由一对 VLAN ID 与 MAC 地址所组成. MFDB 使得两种不同的第二层多播协议可同时在相同的网络设备上作用.MFDB 保持一 VLANID-MAC 地址列表给多重用户组件间共享, 这些组件包含 Static MAC Filtering, GARP Multicast Registration Protocol(GMRP),与 Internet Group Management Protocol(IGMP) Snooping.

- **MAC 地址 —** 此栏位用以指定将在多播转发数据表中搜导的 MAC 地.
- **多播转发数据库列表** —此表显示所有端口所学习到的信息,这些信息包含

  MAC 地址 - 交换机已转发或过滤信息的多播 MAC 地址.格式是由冒号分离的 8 个两位十六进制数.例如:01:23:45:67:89:AB:01:01.
  组件 - 多播转发数据库组件这些组件，包含 Static MAC Filtering, GARP Multicast Registration Protocol(GMRP), 与 Internet Group Management Protocol(IGMP) Snooping.
  类型 - 此栏位显示 MAC 地址的类型，其值 Static 或 Dynamic.Static。表示为用户所设定的MAC地址.Dymamic为经由一些学习 程序或协议而加入此表中,例GMRP IGMP Snooping.
  端口 - 对所选地址作指定的转发或过滤的所有端口.
  端口总结 - 端口总结是由所有转发端口的总和并减去所有静态过滤端口的结果.

5.4 设置 IP 地址配置

指向指示灯面板之下的菜单选项, 点击标签’**IP** 配置’ , 将出现以下屏幕.

5.4.1 设置 IP 地址配置(IP Address)

图 **5-9** IP 地址配置



网络配置协议—此栏定义哪种网络配置协议被使用。如果你修改此值，改变会立刻生效。**bootp** 表示交换机周期性地送请求到 BootP 服务器或 **dhcp** 服务器直到收到答复,**none** 表示交换机手工配置 ip 地址。

IP地址—此栏设定交换机的IP地址.

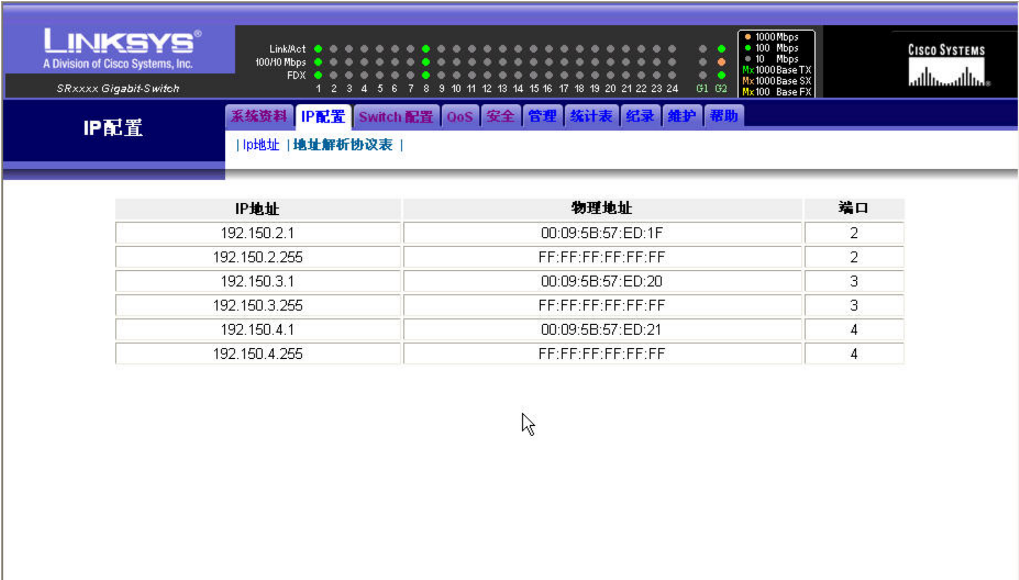
掩码 —此栏设定交换机的子网掩码.

预设网关—此栏设定交换机的网关。IP 地址和网关必须是在同一子网。

注: 变动当前的 IP 地址的将导致在主机和交换机之间当前的连接被中断。变动之前应确定需要新 IP 地址。

5.4.2 ARP 表**(ARP Table)**

图 **5-10** ARP Table 屏幕



此窗口显示交换机和其它设备之间的连通性。地址解析协议(ARP) 高速缓存所辨认与交换机通讯 IP 工作站的 MAC 地址。

IP 地址 **—**从各个端口学到的 IP 地址.

MAC 地址**—**交换机已转发并且/或者过滤信息的点播 MAC 地址。格式是由冒号分开的 6 个两位十六进制数，例如 01:23:45:67:89:AB.

Port —端口编号.

5.5 设置交换机配置

设置交换机配置，指向菜单选项并点击标签'**Switch 配置**'。将出现以下屏幕.

图 **5-11** 交换机配置



此屏幕显示各个端口的当前状态表。它包含以下信息:

- **端口配置**—显示或让你配置链接、速度、双工。参见章节 5.5.1 '端口配置'。
- **VLAN** —让你创建，修改，和删除 VLANs 。参见章节 5.5.2 'VLAN 配置'。
- **VLAN 端口** —让你设定 VLAN 各个端口参数。参见章节 5.5.3 '设定 VLAN 端口'。
- **生成树**—让你定义交换机的生成树参数。参见章节 5.5.4 '生成树'。
- **生成树端口配置** —让你定义交换机各个端口的生成树参数。参见章节 5.5.5 '生成树端口配置'。
- **LA 配置** —让你定义链路聚合组的端口。参见章节 5.5.6 ' 链路聚合配置'。
- **端口监测**—让你设定了一个监测端口和一个被监测的端口。参见章节 5.5.7 '端口监测设置'。
- **GARP** —让你查看并且/或者改变生成树配置和端口设定。参见章节 5.5.8 'GARP 配置' 。
- **IGMP 窥探** —让你设定 IGMP Snooping 信息参数。参见章节 5.5.7 'IGMP 窥探'。

5.5.1 端口配置

查看并且/或者改变各个端口，指向菜单选项**’Switch 配置’**并点击’ **端口配置**’。将出现以下屏幕.

图 **5-12** 端口配置



端口# －端口编号

✎ －此列为各个端口选择栏位，用以选择要做变更的端口.

连接(Mbps) －各个端口的当前的连接速度。

端口类型－各个端口的类型。如果不是空白，表示此端口是端口的一个特殊类型。可能的值是：

Mon -此端口是被监测的端口。查看**’端口监测’**屏幕会有更多信息.

Lag -此端口是 LA 的成员。查看**‘LA 配置’**屏幕会有更多信息.

Probe -此端口是探测端口。查看**’端口监测’**屏幕会有更多信息..

速率设定－希望的端口速度.

双工设定－希望的端口模式.

管理控制－各个端口的管理控制模式.

连接 Trap －连接 Trap 方式。此对象决定当连接状态改变时是否发送 Trap。

LACP 模式 －显示各个端口 LACP 是否开启。

利用以下步骤可以配置一个端口或多个端口:

1. 点选一个或多个端口,再点击**'修改选择的端口设定'**按钮。将出现以下屏幕。如果你想要重设为缺省值,你可点击**'复位选择的端口设定成缺省值'**按钮。

图 **5-13** 端口配置屏幕(2)

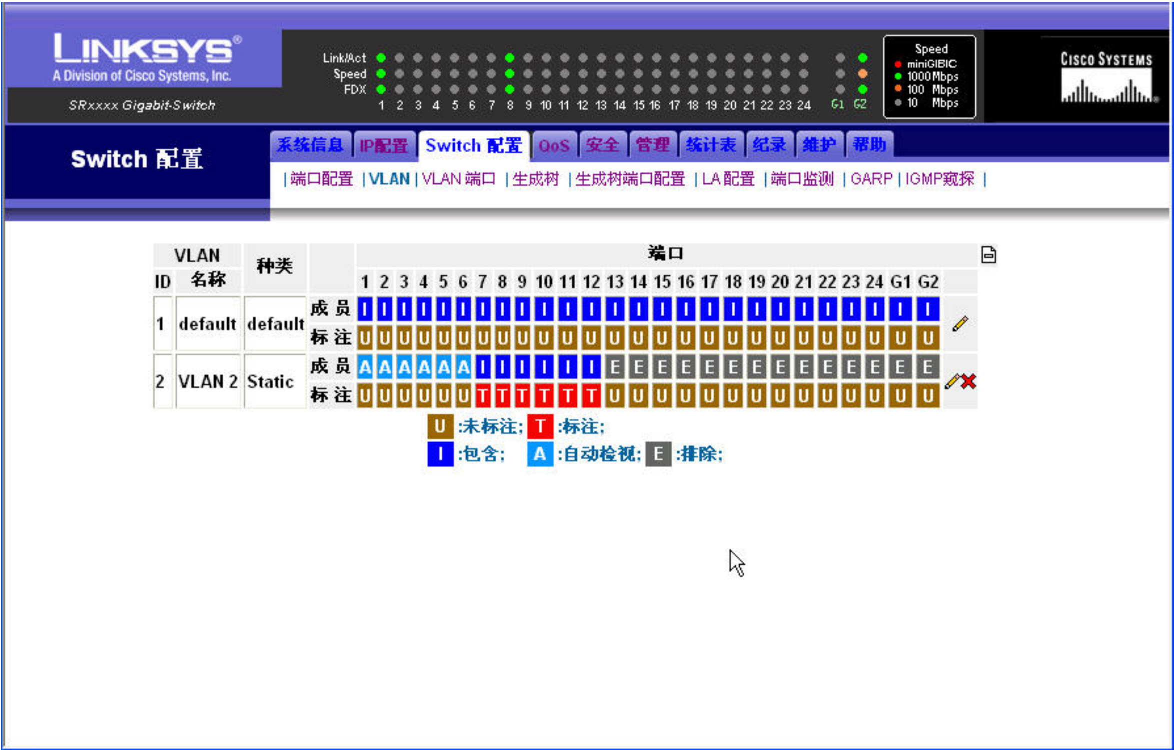


- **实体模式**—此栏让你设置~~子~~希望的端口速度和双工模式。如果选择自动协商，则双工模式和速度将被设置为自动协商。注意端口的最大全双工-100M 将被广告。否则，此对象将决定端口的双工模式和传输速率。工厂缺省值是自动协商。
- **管理模式** —此栏可以使此端口开启或关闭。缺省值为 enable。
- **连接 Trap** —此栏能开启或关闭接口连接状态 Trap。缺省值为 enable。
- **LACP Mode** —此栏可以在端口开启或关闭链路聚集协议（LACP）。缺省值为 enable。

5.5.2 VLAN 配置

查看并且/或者改变 VLANs，指向菜单选项并点击 **VLAN** 。VLAN 设置的状态显示如以下视窗。

图 **5-14** VLAN 配置



此屏幕中的图标被定义如下：

' 🗎 ' –创建新 VLAN
' ✎ ' – 修改存在的 VLAN
' ✖ ' – 删除 VLAN

注:任一已经被定义 VLAN 的 VLAN ID 和名称如上图显示。VLAN 1 为工厂缺省数字，无法被删除。

成员栏位表示各个端口的参与选择。参与选择有:

包含 该接口永远为此 VLAN 成员，相当于固定注册.
排除 该接口永远不为此 VLAN 成员，相当于不许注册.
自动侦测 该接口由 GVRP 动态注册到此 VLAN. 此接口不会加入此 VLAN 成员除非由此界面收到一个

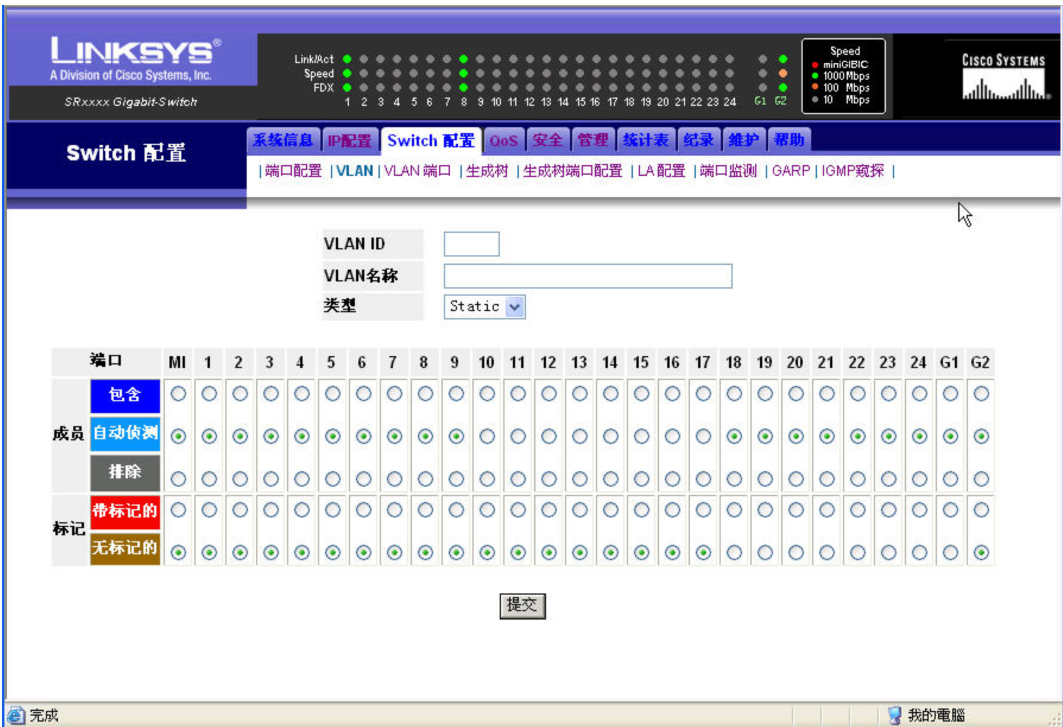
加入要求,这相当于正常注册.

标记栏表示在 VLAN 中一个特定接口的标记行为。如果标记是 enable,信息流量以带标记的 frame 传送。如果标记是 diable 的，信息流量以不带标记的 frame 传送。

创建/修改一个 VLAN

创建或修改 VLAN 时将显示以下屏幕。

图 **5-15** VLAN 配置



VLAN ID — VLAN 的识别号。ID 为 1 是保留给缺省 VLAN 的。VLAN 范围是 2 - 4096.

VLAN 名称 — VLAN 的名称。是 16 个字母与数字的字符串。

类型 — 此栏位改变动态创建的 VLAN(由 GVRP 注册创造)成一个静态 VLAN (一个永久被配置和被定义的) 。

成员 — 使用圆钮选择各个端口参与特定 VLAN 的方式。

标记— 使用圆钮选择是否开启 VLAN 端口的标记行为。

5.5.3 设置 VLAN 端口

配置 VLAN 端口，指向菜单选项**’Switch 配置’**并点击 VLAN 端口。将显示出一个与下面图示相似的屏幕.

图 **5-16** VLAN 端口配置屏幕



端口 #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	2(
链接 Mbps	N/A	N/A	100	N/A	N/A	N/A	N/A	100	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/
端口种类					Lag	Lag	Lag	Lag			Mon	Mon								
速率设置	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Au
双工设置	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Au
信息流控制设置	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Ena
管理控制	On	On	On	On	On	On	On	On	On	On	On	On	On	On	On	On	On	On	On	O
生成树协议状态	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Ena
链接自陷	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Ena
链路聚合模式	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Ena

此屏幕显示 VLAN 端口信息。

- **PVID** — 此端口将指定给不带标记的frame或priority tagged frame的VLAN ID, 此值必须是现存的VLAN.工厂缺省值是1。
- **可接受的Frame类型** — 定义在此端口可能被收到的frame类型.选项有’VLAN only’和’Admit All’.当设成’VLAN only’时, 在此端口收到的不带标记的帧或priority tagged frame会被丢弃。当设置成’Admit All’时, 在此端口收到的不带标记的frame或priority tagged frame会被接受且被指定此端口的VLAN ID值。对任一种选项带标记的帧将依802.1Q VLAN标准转送。
- **只接收VLAN ID相符的分封** — 可能为enabled或disabled.当设成enabled时,此帧相关的端口不是此VLAN的成员,则此帧会被丢弃.对带标记的frame中是以标记中的VLAN ID来识别VLAN.对不带标记的帧,VLAN就是收到该帧所被指定的端口VLAN ID.当设成disabled时,所有的帧依802.1Q VLAN标准转送。工厂缺省值是disabled。
- 点击端口编号以选择该端口配置它的VLAN 参数，如下面图示。端口MI指的是交换机的管理界面端口。

图 **5-17**



- **端口 VLAN ID** —一个下拉菜单列出所有现有的 VLAN 。此栏改变该特定接口的 VLAN ID.
- **可接受 Frame** 类型—此栏设定该特定接口可接受的帧类型.
- **只接收 VLAN ID 相符的分封** —此栏将开启或关闭该特定接口的 Ingress Filtering 功能。如果 Ingress Filtering 功能被关闭, 收到的帧其 VLAN ID 虽与该接收接口所属的 VLAN 不符,仍会被接受并转发到该 VLAN 成员的端口.

5.5.4 生成树配置

配置链路集合，指向菜单选项**'Switch 配置'**并点击**'生成树'**。显示如以下窗口。

图 5-18

Switch 配置

系统信息 | IP配置 | Switch 配置 | QoS | 安全 | 管理 | 统计表 | 纪录 | 维护 | 帮助

| 端口配置 | VLAN | VLAN 端口 | 生成树 | 生成树端口配置 | LA 配置 | 端口监测 | GARP | IGMP窥探 |

Spanning Tree Admin Mode	Disable
Force Protocol Version	IEEE 802.1s
Configuration Name	00-03-6D-00-00-02
Configuration Revision Level	0 (0 to 65535)
Configuration Digest Key	0xac36177f50283cd4b83821d8ab26de62
CST Bridge Identifier	80:00:00:03:6d:00:00:02
CST Bridge Priority	32768 (0 to 61440)
CST Bridge Max Age	20 (6 to 40)
CST Bridge Hello Time	2 (1 to 10)
CST Bridge Forward Delay	15 (4 to 30)
CST Time Since Topology Change	0 day 0 hr 0 min 0 se
CST Topology Change Count	0
CST Topology Change	False

- **Spanning Tree Admin Mode**－生成树管理的模式，开启或关闭.
- **Force Protocol Version** －所使用生成树协议的版本.可选择IEEE 802.1d, IEEE 802.1w, IEEE 802.1s之一.
- **Configuration Name** －此生成树协议配置名称.
- **Configuration Revision Level** －此生成树协议配置版本.
- **Configuration Digest Key** －显示Digest Key.
- **CST Bridge Identifier** －显示Bridge Identifier
- **CST Bridge Priority** －配置Bridge Priority
- **CST Bridge Max Age** －配置CST Bridge Max Age
- **CST Bridge Hello Time** －配置CST Bridge Hello Time
- **CST Bridge Forward Delay** －配置CST Bridge Forward Delay
- **CST Time Since Topology Change** －显示CST Time Since Topology Change
- **CST Topology Change Count** －显示CST Topology Change Count
- **CST Topology Change** －显示CST Topology Change
- **CST Designated Root** －显示CST Designated Root
- **CST Root Path Cost** －显示CST Root Path Cost
- **CST Root Port** －显示CST Root Port
- **Max Age(secs)** －显示Max Age
- **Forward Delay(secs)** －显示Forward Delay

- **Hold Time(secs)** 一显示Hold Time
- **CST Regional Root** 一显示CST Rigional Root
- **CST Path Cost** 一显示CST Path Cost

此屏目亦显示所配置的多生成树的信息，其中包含:

- **MST ID**
- **MST Bridge Priority**
- **Time Since Topology Change**
- **Topology Change Count**
- **Topology Change**
- **Designated Root**
- **Root Path Cost**
- **Root Port**
- **FID**
- **VLAN ID**

若要新增一多生成树，点击图标' 🗎 '即会出现如下屏幕:

图 5-19



- **MST ID**一配置多生成树 ID

接着输入此多生成树的参数，出现如下屏幕

图 5-20

- MST ID
- Priority
- VLAN ID
- Bridge Identifier
- Time Since Topology Change
- Topology Change Count
- Topology Change
- Designated Root
- Root Path Cost
- Root Port

5.5.5 生成树端口配置

对配置生成树端口，指向菜单选项**'Switch配置'**并点击**'生成树端口配置'**。显示如下视窗。

图 5-21

Switch 配置

系统信息 | IP配置 | Switch 配置 | QoS | 安全 | 管理 | 统计表 | 纪录 | 维护 | 帮助

|端口配置 |VLAN |VLAN 端口 |生成树 |生成树端口配置 |LA 配置 |端口监测 |GARP |IGMP窥探 |

Spanning Tree Admin Mode	Disable
Force Protocol Version	IEEE 802.1s
Configuration Name	00-03-6D-00-00-02
Configuration Revision Level	0 (0 to 65535)
Configuration Digest Key	0xac36177f50283cd4b83821d8ab26de62
CST Bridge Identifier	80:00:00:03:6d:00:00:02
CST Bridge Priority	32768 (0 to 61440)
CST Bridge Max Age	20 (6 to 40)
CST Bridge Hello Time	2 (1 to 10)
CST Bridge Forward Delay	15 (4 to 30)
CST Time Since Topology Change	0 day 0 hr 0 min 0 se
CST Topology Change Count	0
CST Topology Change	False

- **MST ID**－配置MST ID
- 端口－配置端口
- **Port Priority**－配置Port Priority
- **Admin Edge Port**－配置Admin Edge Port
- **Port Path Cost**－配置Port Path Cost
- **Auto-calculate Port Path Cost** －显示Auto-calculate Port Path Cost
- **Port ID** －显示Port ID
- **Port Up Time Since Counters Last Cleared** －显示 Port Up Time Since Counter Last Cleared
- **Port Mode** －显示Port Mode
- **Port Forwarding State** －显示Port Forwarding State
- **Port Role** －显示Port Role
- **Designated Root** －显示Designated Root
- **Designated Cost** －显示Designated Cost
- **Designated Bridge** －显示Designated Bridge
- **Designated Port** －显示Designated Port
- **Topology Change Acknowledge** －显示Topology Change Acknowledge
- **Hello Time (secs)** －显示Hollo Time
- **Edge Port** －显示Edge Port
- **Point-to-point MAC** －显示Point-to-poing MAC
- **CST Regional Root** －显示CST Regional Root

- **CST Path Cost** －显示CST Path Cost

5.5.6 LA 配置(Link Aggregation Configuration)

对配置链路集合，指向菜单选项**'Switch 配置'**并点击**'LA 配置'**。所有链路集合(LAGs) 概要被显示如以下窗口。

图 5-22



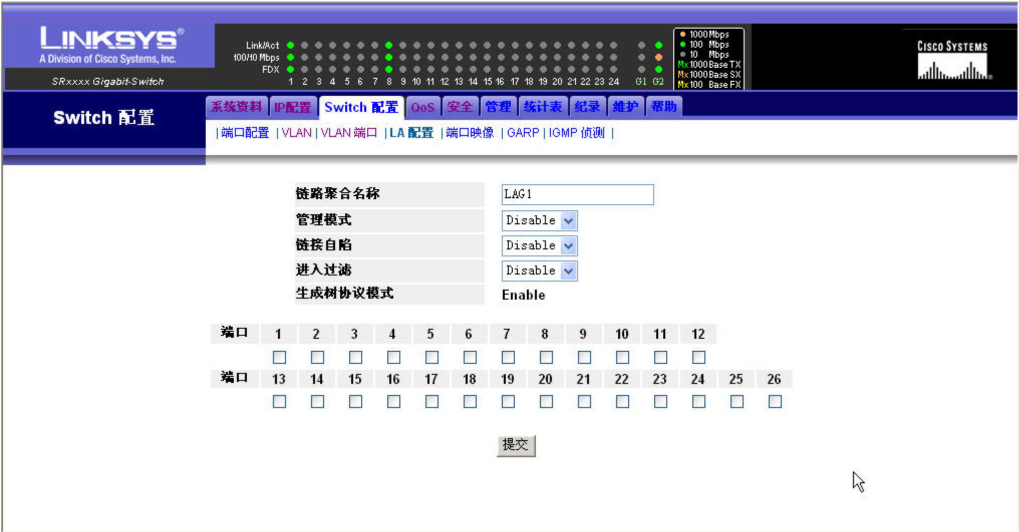
LAG 端口	LAG名称	管理模式	连接状态	Link Trap	STP模式	成员端口
1	LAG1	Enable	Link Up	Enable	Enable	5,6,7,8
2	LAG2	Enable	Link Up	Enable	Enable	11,12,13,14

- **LAG**端口－ 此LAG的逻辑端口.
- **LAG**名称 － 此LAG的名称.
- 连接状态 － 此LAG是否连接.
- 管理模式 －此LAG的管理的模式，开启或关闭.
- **Link Trap** －当连接状态改变时，此对象决定是否发送Trap.工厂缺省值是enabled.
- **STP**模式 －此LAG的STP模式，开启或关闭.
- 成员端口 － 列出的是LAG的成员端口.最多有8个端口指定给LAG.

创建一个新的 LAG 或修改存在的 LAG

创建或修改 LAG ，将出现以下屏幕。

图 5-23



- **LAG** 名称－此 LAG 的名称.
- 管理模式－ LAG 的管理的模式，开启或关闭.
- **Link Trap** － 当连接状态改变时，决定是否发送 Trap.工厂缺省值是 enabled.
- **STP**模式 － 此LAG的STP模式，开启或关闭.
- 成员端口－ 列出所有的实体端口以选择成 LAG 的成员.最多有 8 个端口指定给 LAG.

5.5.7 端口监测

查看或改变端口监测,指向菜单选项**'Switch 配置'**并点击**端口监测**。将出现以下屏幕.

图 5-24

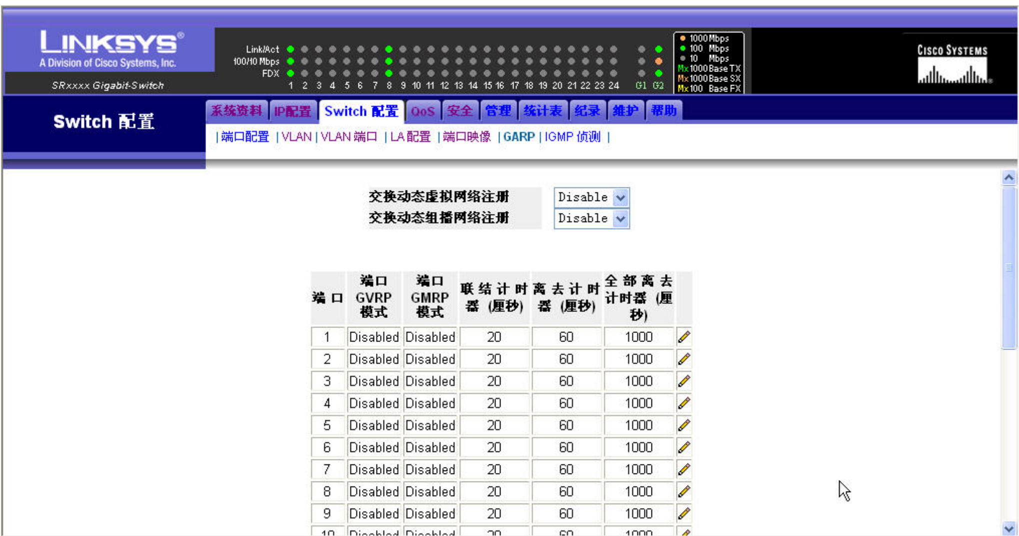


- **探测端口** - 此栏~~位~~指定探测端口.若未指定则显示"Not Configured"..一旦配置好,探测端口将不能网络连接.探测端口将不转发任何信息流量也不接收任何东西.探测工具添加给探测端口将不能去 PING 交换机或者直达交换,任何人都不能 PING 探测工具.
- **被监测端口**- 此栏指定被监测的端口.若未指定则显示"Not Configured".
- **端口监测模式** - 选择端口的监测模式. 它有两种模式 disable 和 enable. 工厂缺省值是 disabled.

5.5.8 GARP 配置

指向菜单选项 **Switch** 配置并点击 **GARP** 。将出现以下屏幕。

图 **5-25** GARP 屏幕



交换机 **GVRP** —此栏位使 GVRP 功能开启或关闭。

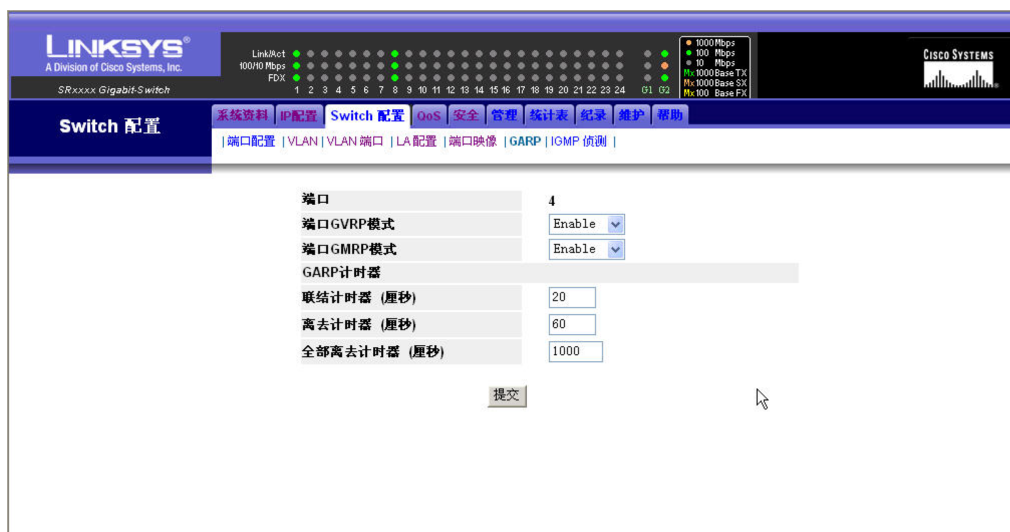
交换机 **GMRP** —此栏位使 GMRP 功能开启或关闭。

GARP 界面表 —此表显示所有界面的 GARP 信息。表中包括

- 端口 **GVRP** 模式 - 指出此端口的 GVRP 管理的模式.它可能是 enabled 或者 disabled..工厂缺省值是 disabled.
- 端口 **GMRP** 模式 - 指出此端口的 GMRP 管理的模式.它可能是 enabled 或者 disabled.工厂缺省值是 disabled.
- 加入周期- 指出间隔之间 GARP PDUs 传送注册时成员资格的属性,当前属性是一个 VLAN 或者多播组.这是此时间在每一个埠,每一个 GARP 参与者基础的一种情况.允许值为 10 到 100 厘秒,工厂缺省值是 20 厘秒.
- 离开周期- 指定此时间的时段去等待然后在接收一个没有注册的属性请求之前清除此请求.当前的属性是一个 VLAN 或者多播组.这是此时间在每一个埠,每一个 GARP 参与者基础的一种情况.允许值为 20 到 600 厘秒,工厂缺省值是 60 厘秒.
- 全部离开周期- 这是 Leave All Timer 控制怎样去经常的要求产生所有 PDUs. Leave All PDU 指出所有注册的.这是此时间在每一个埠,每一个 GARP 参与者基础的一种情况.允许值为 200 到 6000 厘秒,工厂缺省值是 1000 厘秒.

- 配置各个界面GARP 和GMRP 你可以点击特定端口最后一栏的修改图标。以下屏幕将显示.

图 **5-26** GARP 屏幕(2)



- 端口 **GVRP** 模式 - 指出此端口的 GVRP 管理的模式.它可能是 enabled 或者 disabled. 如果选择 disabled,连接时间,离开时间和全离开的时间没有生效.工厂缺省值是 disabled.
- 端口 **GMRP** 模式 - 指出此端口的 GMRP 管理的模式.它可能是 enabled 或者 disabled.如果选择 disabled,连接时间,离开时间和全离开的时间没有生效.工厂缺省值是 disabled.
- 加入周期 - 指出间隔之间 GARP PDUs 传送注册时成员资格的属性,目前属性是一个 VLAN 或者多播组.此时间是每一个埠,每一个 GARP 参与者基础的一种情况.允许值为 10 到 100 厘秒,工厂缺省值是 20 厘秒.
- 离开周期 - 指定此时间的时段去等待然后在接收一个没有注册的属性请求之前清除此请求.当前的属性是一个 VLAN 或者多播组.这是此时间在每一个埠,每一个 GARP 参与者基础的一种情况.允许值为 20 到 600 厘秒,工厂缺省值是 60 厘秒.
- 全部离开周期 - 这是 Leave All Timer 控制怎样去经常的要求产生所有 PDUs. Leave All PDU 指出所有注册的.这是此时间在每一个端口,每一个 GARP 参与者基础的一种情况.允许值为 200 到 6000 厘秒,工厂缺省值是 1000 厘秒.

5.5.9 IGMP 窥探(IGMP Snooping)

查看并且/或者改变 IGMP 窥探配置。指向菜单选项 **Switch 配置**并点击 **IGMP 窥探**。将出现以下屏幕。

图 **5-27** IGMP Snooping Setting

- 管理模式 - 指出在交换机内 IGMP 探测是否有作用.
- 多播群成员区间 - 是指一个交换机将删除一接口项目之前须等待多少秒钟由一特定群组在特定接口的报告.此值须大于 IGMP 最大反应时间的值.范围为 1 到 3600 秒.
- 最大反应时间 - 是指一个交换机因没有收到对一特定群组在特定接口的报告而发出一个要求后要等待的时间.此值要须小于 IGMP 询问周期时间的值.范围为 1 到 3600 秒.
- 多播路由器出现过期时间 - 如果询问在一个接口内部一段时间内没有收到询问,此接口就从自多播路由器付属的接口列表中移除.
- 多播控制 **Frame** 数目 —这显示由 CPU 处理控制的多播帧的数量.
- **IGMP** 窥探界面模式 —此命令使在一特定接口 IGMP 窥探功能开启或关闭.

5.6 服务质量(QoS)

指向指示灯面板之下的菜单选项, 点击标签’**QoS**’ , 将出现以下屏幕.

图 **5-28** QoS 屏幕



- **Diffserv** 配置 —让你开启或关闭 DiffServ 操作状态和显示 DiffServ 一般状态小组信息, 包括目前的行政方式设置并且目前和最大行数在每个主要 DiffServ 私有 MIB 表。参见章节 5.6.1’Diffserv Conf.’ 。
- **Diffserv** 等级－让你配置 Diffserv 等级。参见章节 5.6.2’Diffserv 等级配置’。
- **Diffserv** 策略－让你配置 Diffserv 策略。参见章节 5.6.3’Diffserv 策略’。
- **Diffserv** 服务－让你配置 Diffserv 服务。参见章节 5.6.4’Diffserv 服务’。

5.6.1 Diffserv 配置

设置 DiffServ 运作模式为动作对或不动作和显示 DiffServ 一般状态编组信息,指向菜单选项 **QoS** 并点击 **Diffserv 配置**。将出现以下屏幕。

图 **5-29** Diffserv 配置屏幕



DiffServ 管理模式**—**此栏位设置 DiffServ 运作模式动作对或不动作。其值为 enable 或 disable。缺省值是 disable。当 disable 时, DiffServ 配置仍被保留和可被改变，但它不动作。当 enable 时, Diffserv 服务才动作。

DiffServ 一般状态分组信息表列**—**DiffServ 一般状态分组信息,此表包含括在每个主要 DiffServ 专用 MIB 表的当前容量和最大容量。

- 等级表当前容量　显示当前在等级表中条列的数目。
- 等级表最大容量　显示等级表最大容量。
- 等级规则表当前容量　显示当前等级规则表中条列的数目。
- 等级规则表最大容量　显示等级规则表最大容量。
- 策略表当前容量　显示当前策略表中条列的数目。
- 策略表最大容量　显示策略表最大容量。
- 策略实例表当前容量　显示当前策略实例表中条列的数目。
- 策略实例表最大容量　显示策略实例表最大容量。
- 策略属性表当前容量　显示当前策略属性表中条列的数目。
- 策略属性表最大容量　显示策略属性表最大容量。
- 服务表当前容量　显示当前服务表中条列的数目。

- **服务表最大容量**　显示当前服务表最大容量。

5.6.2 Diffserv Class Configuration

配置 Diffserv 等级，指向菜单选项 **QoS** 并点击 **Diffserv 等级**。将出现以下屏幕。

图 **5-30** Diffserv 等级屏幕



Diffserv 等级表 — 显示用户定义的 Diffserv 等级。此屏幕中的图标定义如下：

'📄' –创建新 Diffserv 等级
'✏' –给特定的 Diffserv 等级增加条件
'✖' – 删除 Diffserv 等级

创建一个 Diffserv 等级

在 DiffServ 中'等级'的被定义为:

流量分类　根据 DSCP, 和流量的 Multi-Field(MF) 等级 (名称,符合条件)（规定 Behavior Aggregate (BA)）

服务水平　规定 BA 转发水平/服务水平。概念上,DiffServ 是有等级的二个阶层：1.服务/PHB, 2.流量等级

等级符合条件或称为等级规则,一个等级定义是由一个或多个规则以认定此流量所属的等级. 注意一旦创建一符合条件给一个等级,它就无法被改变或被删除--整个等级必须被删除和再创建。

创建新等级,点击图标’’。将出现以下屏幕。

图 **5-31** Create a Diffserv Class 屏幕



等级名称 — DiffServ 等级的名称.
等级型类 — Diffserv 等级型类.

增加一个条件到 **Diffserv** 等级

在此屏幕上列出给指定等级的符合条件表。你可在表中选出条件再按’增加符合条件’按钮来增加以一个新的条件给指定的等级。

图 **5-32** 增加一个条件到 Diffserv 等级屏幕



等级符合选择— 这列出你可能选择增加入特定的等级的所有符合条件。符合条件'Every'表示，每个数据报都被考虑符合指定的等级且不须要另外的输入信息。对一指定的等级，基于符合条件选择为'Reference Class'时,此下拉式选择表列会有变化:

- 如果指定的等级不参考其它等级时，'Reference Class'会包含在下拉式选择表中. 等级参考可由下拉式选择表中选择'Reference Class' 再按'增加符合条件'按钮来建立。
- 如果指定的等级参考其它等级时，'Reference Class'就不会包含在下拉式选择表列中. 这可防止用户再增加参考等级, 因为一指定的等级最多只可参考一个同样类型的等级。

以下为每一符合条件的说明。

- **Destination IP Address - Diffserv等级的符合条件**

在指定的等级定义中加入基于目的地 IP 地址的符合条件。

图 **5-33** Destination IP Address – Diffserv 的符合条件屏幕



- **IP 地址** - 此栏指定 Diffserv 的目的地 IP 地址，一个有效的目的地 IP 地址以十进位小数点的格式表示。
- **IP 掩码** - 此栏指定目的地 IP 地址的掩码， 这是一个以十进位小数点的格式表示的 bit mask.用以指示哪一部分的目的地 IP 地址被用为与包的内容相比较.掩码位必须是连续的，以让接口正确地运算，例如 255.128.0.0 是一个合法的 mask， 255.0.128.0 不是一个合法的 mask。

- **Destination Layer 4 Port - Diffserv等级的符合条件**

在指定的等级定义中加入基于分封目的地第 4 层 port 的符合条件。而以一关键字表示法表示此 port。

图 **5-34** Destination Layer 4 Port – Diffserv 的符合条件屏幕

Port Keyword – 此处列出已知目的地第 4 层 port 的关键字作为选择. 若选'other',则在下一栏输入无名称的端口。

- **Destination MAC Address - Diffserv等级的符合条件**

在指定的等级定义中加入基于数据包目的地 MAC 地址的符合条件。

图 **5-35** Destination MAC Address – Diffserv 的符合条件屏幕

- **MAC Address -** 第二层的 MAC 地址格式是 6 个两位十六进制数，以冒号来分开,其缺省值是 00:00:00:00:00:00.
- **MAC Mask -** 第二层的 MAC 地址 bit mask,格式是 6 个两位十六进制数,不能是相邻的,而以冒号来分开,其缺省值是 00:00:00:00:00:00.

- **Every - Diffserv等级的符合条件**

在指定的等级定义中加入的符合条件,基于此所有数据包都属于此等级。

- **IP DSCP - Diffserv等级的符合条件**

在指定的等级定义中加入基于数据包中 IP DiffServ Code Point (DSCP) 栏的值的符合条件。此 IP DiffServ Code Point (DSCP) 栏被定义为在 IP 报头中服务类型八位字节的六个高值位(二个位低值位不被检查) 。

图 **5-36** IP DSCP – Diffserv 的符合条件屏幕

- **DSCP Keyword -** 此处列出已知的 DSCP 值作为选择. 此 DSCP 值(关键字)包含: 10(af11), 12(af12), 14(af13), 18(af21), 20(af22), 22(af23), 26(af31), 28(af32), 30(af33), 0(be), 0(cs0), 8(cs1), 16(cs2), 24(cs3), 32(cs4), 40(cs5), 48(cs6), 56(cs7), 46(ef).

注: ipdscp 、ipprecedence, 和 iptos 符合条件都是供选择的方式，用以指定 Diffserv 等级的符合条件. 都是对 IP 中相同的服务类型为样服务类型栏位, 但与用户在表示法上稍有差异。

- **IP Precedence - Diffserv等级的符合条件**

在指定的等级定义中加入基于数据包中 IP 优先权栏的值的符合条件。该栏被定义为在 IP 报头服务类型八位字节的三个高值位(五个低值位不被检查）。

图 **5-37** IP Precedence – Diffserv 的符合条件屏幕

Precedence Value -此栏位定义 IP 优先权,其值在范围 0 到 7 间作比较。

注: ipdscp 、ipprecedence, 和 iptos 符合条件都是供选择的方式用以指定 Diffserv 等级的符合条件. 都是对 IP 中相同的服务类型为样服务类型栏位, 但与用户在表示法上稍有差异。

- **IP TOS - Diffserv等级的符合条件**

在指定的等级定义中加入基于数据包中 IP TOS 栏的值的符合条件。该栏被定义为在 IP 报头中服务类型八位字节的全部八个值位。

图 **5-38** IP TOS – Diffserv 的符合条件屏幕



TOS Bits -这是 IP TOS 的值为 0 至 FF (十六进制),在与 TOS Mask 的值作 mask 后用来比较。

TOS Mask – 表示在 TOS Bits 中 bit 的位置，被用已与分封中 IP TOS 栏位相比较。

注：ipdscp 、ipprecedence, 和 iptos 符合条件都是供选择的方式用以指定 Diffserv 等级的符合条件. 都是对 IP 中相同的服务类型为样服务类型栏位，但与用户在表示法上稍有差异。

注：实质上，这是 IP DSCP/Precedence/TOS 符合规格的'自由形式'版本，因为用户可完全控制指定 IP 服务类型栏位的哪些 bit 被检查。

- **Protocol - Diffserv等级的符合条件**

在指定的等级定义中加入基于数据包 IP 协议的符合条件。而以一关键字表示法表示此协议。

图 **5-39** Protocol – Diffserv 的符合条件屏幕

协议关键字 -此处列出知名协议的关键字作为选择。若选'other',则在下一栏位输入一数字给无名称的协议。若选'ip',则表示要符合所有协议的值。

- **Reference Class - Diffserv等级的符合条件**

在指定的等级定义中加入定义给另一等级的符合条件集合。

图 **5-40** Reference Class – Diffserv 的符合条件屏幕

参考等级 -此处列出所有现有的同类型的 DiffServ 等级名称，以作为选择给指定的等级。此指定的等级无法参考自己。每一等级定义只允许有一参考等级。

- **Source IP Address - Diffserv 等级的符合条件**

在指定的等级定义中加入基于数据包的源 IP 地址的符合条件。

图 **5-41** Source IP Address – Diffserv 的符合条件屏幕

- **IP 地址** - 此栏位指定 Diffserv 的源 IP 地址，一个有效的源 IP 地址以十进位小数点的格式表示。
- **IP 掩码** - 此栏位指定源 IP 地址的掩码， 这是一个以十进位小数点的格式表示的 bit mask. 用以指示哪一部分的源 IP 地址被用为与数据包的内容相比较. mask bit 必须是连续的，以让接口正确地运算，例如 255.128.0.0 是一个合法的 mask，255.0.128.0 不是一个合法的 mask。

- **Source Layer 4 Port - Diffserv等级的符合条件**

在指定的等级定义中加入基于数据包来源第 4 层 port 的符合条件。而以一关键字表示法表示此 port。

图 **5-42** Source Layer 4 Port – Diffserv 的符合条件屏幕

Port Keyword – 此处列出已知来源第 4 层 port 的关键字作为选择. 若选'other',则在下一栏位输入无名称的 port。

- **Source MAC Address - Diffserv等级的符合条件**

在指定的等级定义中加入基于数据包源 MAC 地址的符合条件。

图 **5-43** Source MAC Address – Diffserv 的符合条件屏幕

- **MAC Address -** 第二层的 MAC 地址格式是 6 个两位十六进制数以冒号来分开,其缺省值是 00:00:00:00:00:00.
- **MAC Mask -** 第二层的 MAC 地址 bit mask,格式是 6 个两位十六进制数,不能是相邻的,而以冒号来分开,其缺省值是 00:00:00:00:00:00.

- **VLAN - Diffserv等级的符合条件**

在指定的等级定义中加入基于数据包的第二层 VLAN ID 栏位的值的符合条件。

图 **5-44** VLAN – Diffserv 的符合条件屏幕



VLAN Identifier -此栏位 VLAN 标识符, 其值在 1 到 4094 范围作为比较。

5.6.3 Diffserv 策略配置

设置 DiffServ 策略，在菜单选项 **QoS** 并点击 **Diffserv Policy**。将出现以下屏幕。

图 **5-45** Diffserv Policy 屏幕



DiffServ 策略信息表—显示用户定义的 Diffserv 策略。此屏幕中的图标表示如下:

' ' –创建造新 Diffserv 策略
' ' –修改 Diffserv 策略
' ' –删除Diffserv策略

创建一项 **Diffserv** 策略

在 DiffServ 中策略被用以定义:
流量状况 指定流量状况的动作(policing, marking,shaping) 来用于流量等级
服务规范 指定服务水平(EF,AF,等)的带宽和队列长度管理要求。

策略被用来将一个流量等级与一个或多个 QoS 策略属性关联在一起,此流量等级是在 Diffserv 等级定义。此关联然后被分配到一个接口在一个特殊方向形成一个服务。当策略被创建时用户指定策略名称。
它不一定要求用户只将一流量与一个策略关联在一起。实际上，多个流量等级可与一个策略关联在一起,每一种流量等级定义一种特殊处理方式给符合等级定义的数据包。当一个数

据包满足超过一个等级的条件时，其优先级是基于等级添加到策略的先后，最先的采取最高的优先权。

注意唯一的方式去从一个策略中的等级事例将一个单独策略属性移除就是将此等级事例移除再重新把它加到策略。与一个现有的策略属性关联的值不须移除等级事例即可被改变。

创建一项新 Diffserv 策略点击图象' '将出现以下屏幕。

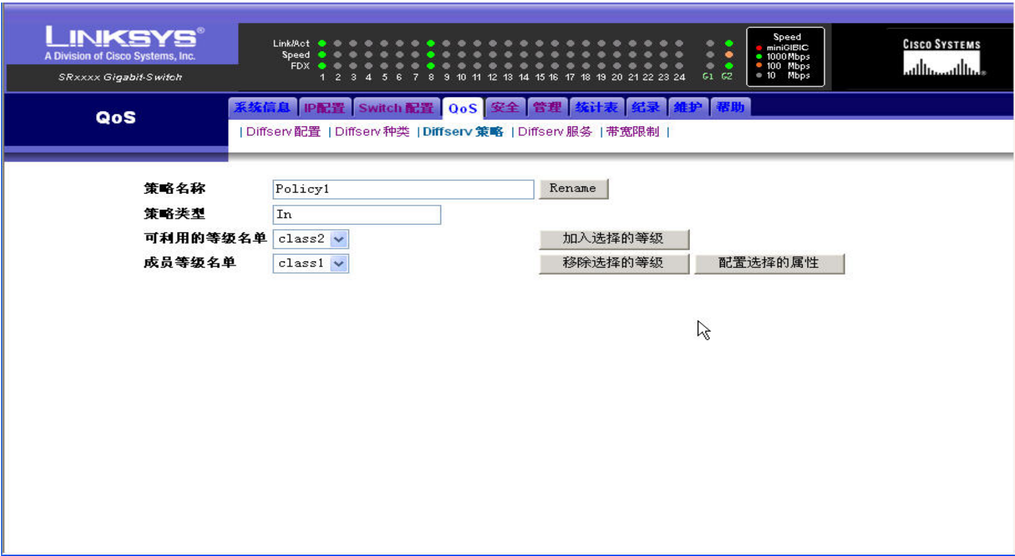
图 **5-46** 创造一 Diffserv 策略屏幕

- **策略名称—**Diffserv 策略的名称。这是一个字符串，以 1 到 31 个有大小写区分的字母数字所组成，字符独一地识别此策略。
- **策略类型—**此栏位定义流量方向是向内或向外。

Diffserv 等级与 Diffserv 策略关联

在创造 Diffserv 策略以后你需要将 Diffserv 等级与它关联。将出现以下屏幕。

图 5-47 Diffserv 等级与 Diffserv 策略关联屏幕

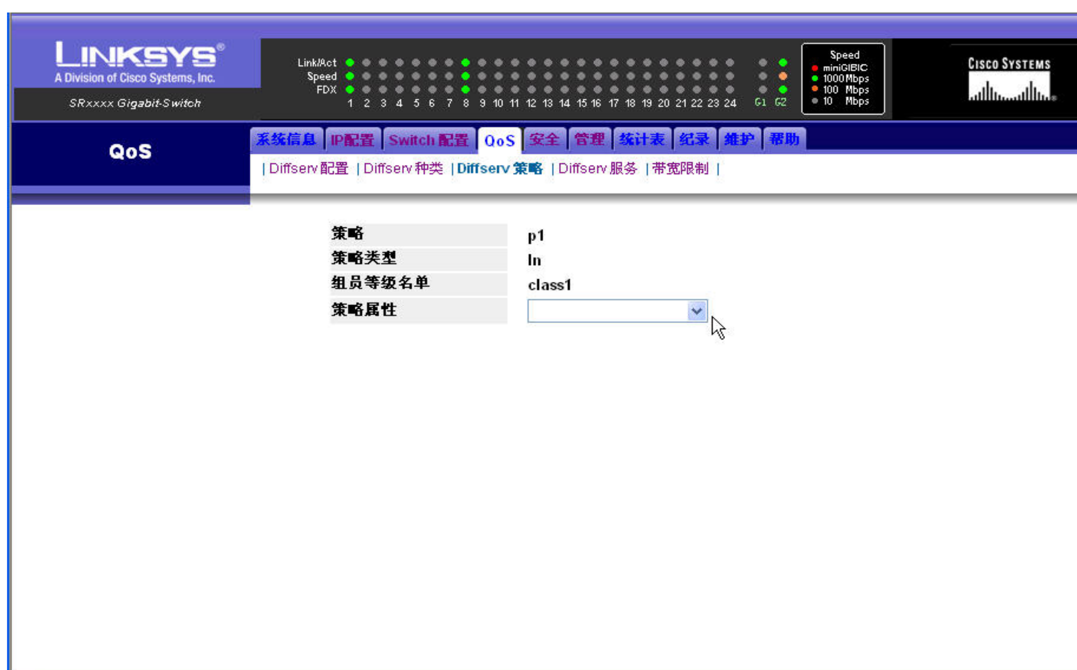


- **可利用的等级名单**—此栏位列出所有现有的 DiffServ 等级名单，以供选择加入指定的策略。
- **成员等级名单**—此栏位列出所有现有被定义作为指定的策略的成员 Diffserv 等级名单，以供选择由指定的策略中移除。

配置属性给一 Diffserv 策略

在将等级与 Diffserv 策略关联后对你需要配置属性给指定的策略。将出现以下屏幕。

图 **5-48** 配置属性给指定的策略屏幕



策略属性 —此栏位列出这类型策略所支持的所有属性，这些属性包括 Mark IP DSCP, Mark IP Precedence 和 Police Simple.每一种属性需要作更进一步配置。

配置属性’Mark IP DSCP’给 Diffserv 策略

此属性在所有相关连信息流数据包中加入指定的 IP DSCP 值的标记.

图 5-49　配置属性’Mark IP DSCP’给 Diffserv 策略屏幕



DSCP 关键字 —此处列出已知的 DSCP 值作为选择.此 DSCP 值(关键字)包含: 10(af11), 12(af12), 14(af13), 18(af21), 20(af22), 22(af23), 26(af31), 28(af32), 30(af33), 0(be), 0(cs0), 8(cs1), 16(cs2), 24(cs3), 32(cs4), 40(cs5), 48(cs6), 56(cs7), 46(ef).

配置属性’Mark IP Precedence’给 Diffserv 策略

此属性在所有相关连信息流数据包中加入指定的 IP Precedence 值的标记.

图 **5-50** 配置属性'Mark IP Precedence'给 Diffserv 策略屏幕

IP Precedence 值 —IP Precedence 值是一个从 0 到 7 的整数。

配置属性'Police Simple'给 Diffserv 策略

Police Simple策略属性是一种方法管理调节信息流的设备的方法,它被用来建立监管型式给指定等级.流量被以一单一速率与burst大小监管.其结果有两者:遵守(conform)与不遵守(noconform). 遵守的数据被以kilobits-per-second(Kbps)定义,其值为 1 到 4294967295 的整数.遵守的burst大小被以kilobytes (KB) 定义,其值为 1 到 128 的整数.

对每一结果只有一种可能的动作为Send, Drop, Mark IP DSCP,或 Mark IP Precedence.

在此Police Simple策略属性中遵守的动作缺省值为Send与不遵守的动作缺省值为Drop.

若遵守/不遵守的动作为Marked IP DSCP Marked IP Precedence时,还须设定其值.

图 **5-51** 配置属性'Police Simple'给 Diffserv 策略屏幕

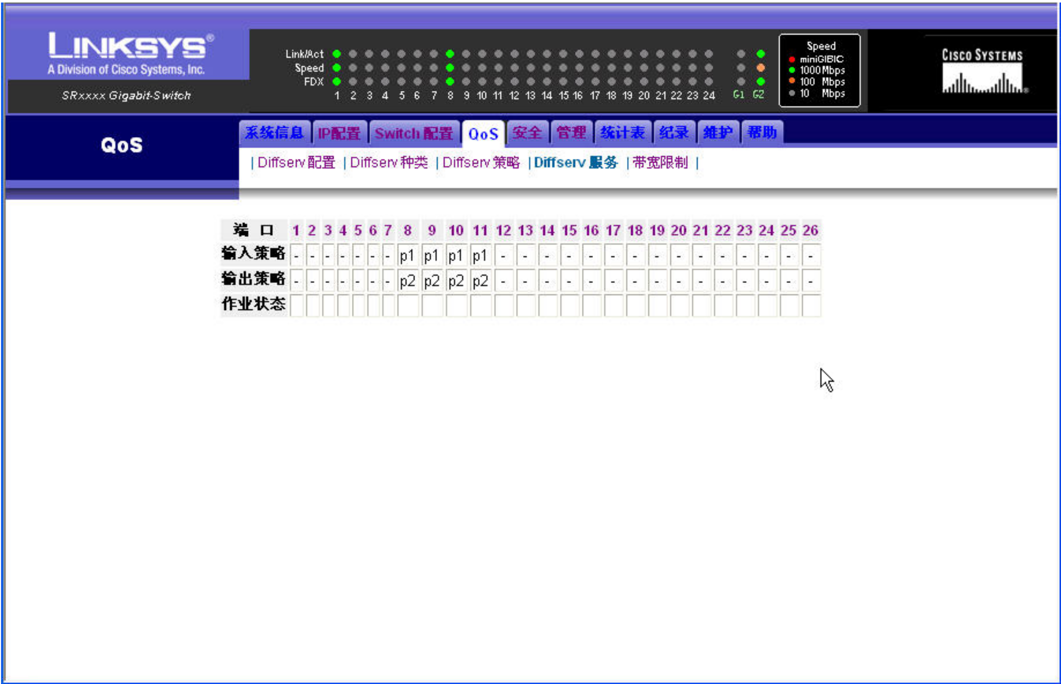


- **Conform** 的动作 —设定在此策略指定等级中遵守监管流量的动作. 此动作的值为 Send, Drop, Mark IP DSCP,或 Mark IP Precedence. 缺省值为 Send。
- **Non-Conform** 的动作 —设定在此策略指定等级中不遵守监管流量的动作. 此动作的值为 Send, Drop, Mark IP DSCP,或 Mark IP Precedence. 缺省值为 Drop。
- 承诺的速率 **(kbps)** —承诺的数据被以 kilobits-per-second(Kbps)定义, 其值为 1 到 4294967295 的整数。
- 承诺的 **Burst** 大小**(KB)** —承诺的 Burst 大小被以 kilobits-per-second(Kbps)定义, 其值为 1 到 128 的整数。

5.6.4 Diffserv Service

Diffserv 服务就是将 Diffserv 策略运用在一个界面的一个特殊方向。设置 DiffServ 服务指向菜单选项 **QoS** 并点击 **Diffserv Service**。将出现以下屏幕。

图 **5-52** Diffserv 服务屏幕



端口	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
输入策略	-	-	-	-	-	-	-	p1	p1	p1	p1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
输出策略	-	-	-	-	-	-	-	p2	p2	p2	p2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
作业状态																										

- **服务表—**显示每一界面在in方向和out方向所相关联的策略. 点击欲设定的端口以便将现有的与此端口关联.

端口　　接口的端口编号。

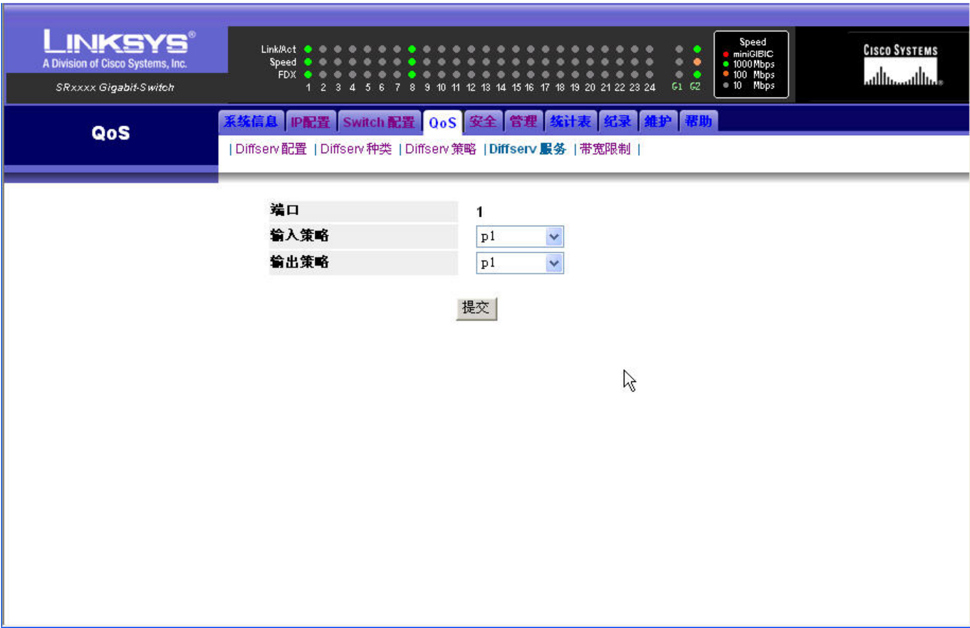
输入策略　指定界面在’In’方向关联的策略。

输出策略　指定界面在’Out’方向关联的策略。。

配置一项服务给一个指定端口

配置一项服务给一个指定端口，点击欲设定的端口编号。将出现以下屏幕。

图 **5-53** 配置一 Diffserv 服务给一个指定端口屏幕



- **输入策略—**此栏位列出将被选择给一个指定端口（在 In 方向现有的策略名单）。
- **输出策略—**此栏位列出将被选择给一个指定端口（在 Out 方向现有的策略名单）。

5.6.5 带宽限制

设置带宽限制。指向菜单选项 **QoS** 并点击**带宽限制**。将出现以下屏幕。

图 **5-54** 带宽限制屏幕



● **带宽限制表—**显示每一界面的带宽限制.若无限制则为该端口最大线速。

入口处带宽　指定界面在'In'方向关联的带宽限制速率。

出口处带宽　指定界面在'Out'方向关联的带宽限制速率。

点击端口图像'　' 以配置该端口带宽,或点击图像'　' 以重置端口带宽为线速。

配置端口带宽将出现以下屏幕

图 **5-55** 带宽限制配置屏幕

端口	5
入口处带宽 (Mbps)	0
出口处带宽 (Mbps)	0

提交

入口处带宽　指定接口在'In'方向关联的带宽限制速率。

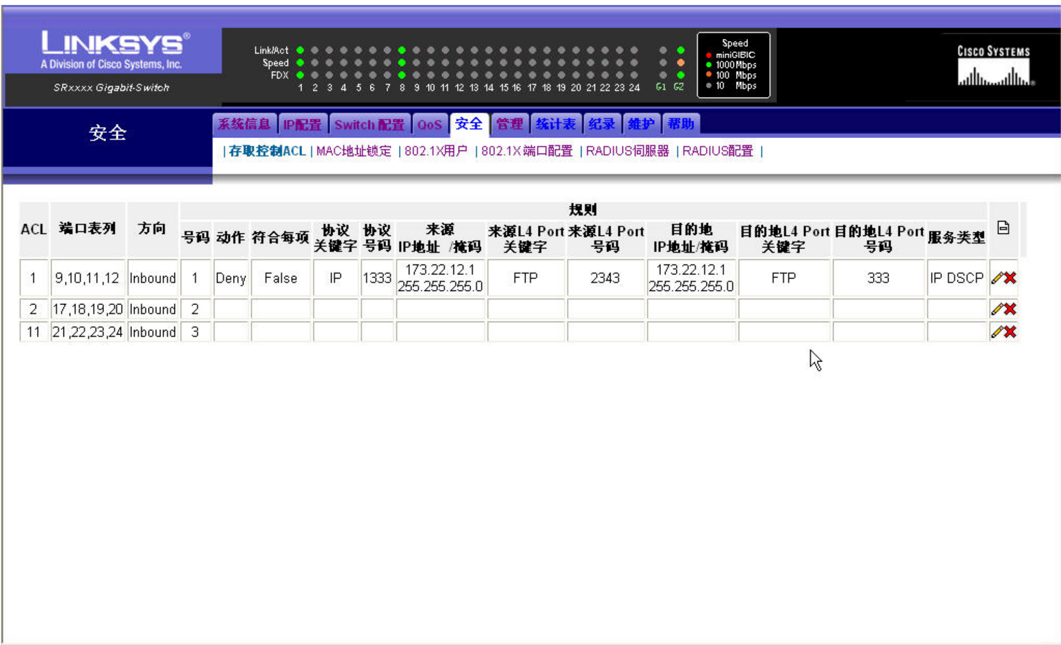
出口处带宽　指定接口在'Out'方向关联的带宽限制速率。

对于各个百兆位端口其带宽限制步长为 1Mbps，对于各个千兆位端口其带宽限制步长为 8Mbps。

5.7 安全配置

指向指示灯面板之下的菜单选项, 点击标签 ’**安全**’, 将出现以下屏幕.

图 **5-56** 安全配置屏幕



- 存取控制**ACL —** 让你查看和配置Access Control List。参见章节5.7.1 ’存取控制ACL’。
- **MAC**地址锁定**—** 让你配置MAC地址锁定。参考章节5.7.2 ’ MAC地址锁定’。
- **802.1X**用户**—** 让你配置802.1X 用户。参考章节5.7.3 ’802.1X 用户’。
- **802.1X**端口配置 **—** 让你配置802.1X 端口,参考5.7.4 ’802.1X 端口配置’。
- **RADIUS**服务器 **—** 让你配置RADIUS服务器的信息。参考章节5.7.6 ’ RADIUS 服务器’。
- **RADIUS**配置 **—** 让你配置RADIUS。参考章节5.7.5 ’RADIUS配置’。

5.7.1 存取控制 ACL

存取控制 ACL 确保只有认可的用户可访问指定的资源且阻挡任何非法欲接近网络资源者.
要配置访问控制表,指向菜单选项'安全'并点击'**存取控制 ACL**'。将出现以下屏幕。

图 **5-57** 安全配置屏幕



与系统相关联的访问控制列表(ACL) 总结表显示于此页。其中包括下列信息

ACL —此栏位显示 ACL 号码. 它是 1 到 99 的整数. 范围由 1 到 99 为标准的 AC L 列表, 范围由 100 到 199 为扩展的 ACL 列表. 一般的 ACL 列表只允许源 IP 地址/掩码配置, 扩展的 ACL 表列则可配置协议, 源 IP 地址/掩码, 源 Port, 目的地 IP 地址/掩码, 目的地 Port, 符合的服务等级, 符合的服务等级值。

端口表列 —此栏位显示与此 ACL 相关联的端口。

方向 —此栏位显示在此接口 ACL 过滤方向。可能的值是'inbound'。

Rule —此栏位显示与此 ACL 相关联的规则。关于规则的信息包括

- 号码 - 此号码为每一与 ACL 相关联的规则的识别号码。
- 动作 - 此栏位为每一规则相关联的动作。可能的值是 Deny 或 Permit。
- 符合每项 – 指定一符合条件,此条件中所有数据包都符合 ACL 及规则号码所定义的 ACL 规则. 其值为 False 或 True.
- **来源 IP 地址**– 指定来源 IP 地址给此规则
- **来源 IP 掩码** – 指定来源 IP 掩码给此规则.
- 目的地 **IP** 地址 - 指定目的地 IP 地址给此规则
- 目的地 **IP** 掩码 – 给此规则指定目的地 IP 的掩码.
- **来源 L4 Port** 关键字 - 此规则指定来源第四层 port 符合条件
- **来源 L4 Port** 号码 -给此规则指定来源第四层 port 符合条件. 其值为 0 到 65535.

- **目的地 L4 Port 关键字** - 指定目的地第四层 port 符合条件给此规则.
- **目的地 L4 Port 号码** - 指定目的地第四层 port 符合条件给此规则. 其值为 0 到 65535.
- **协议关键字** – 指定协议给此规则过滤, 可能的值为 IGMP, ICMP, IP, TCP, UDP.
- **协议号码** – 指定协议号码与此 ACL 关联
- **服务类型** -指定服务类型为 IP DSCP, IP Precedence, 或 IP TOS 符合条件给此规则.

此屏幕中的图标被定义于下面:

' ' – 创建新存取控制表
' ' – 修改存取控制表
' ' – 删除存取控制表

创建/修改 Access Control List

点击 Access Control List 总结表中的图标' ' 或' '将出现以下屏幕。

图 **5-58** 创造 Access Control List 屏幕

ACL ID	1
选择的端口(s)	3,4,5
方向	Inbound
规则选择	Create Rule
规则	0 (1 - 10)
动作	Deny
符合每项	False
来源IP地址 来源IP掩码	192.168.2.1 255.255.255.0
目的地IP地址 目的地IP掩码	192.168.2.1 255.255.255.0
来源L4 Port关键字	ftp
来源L4 Port号码	21 (0 - 65535)
目的地L4 Port关键字	other
目的地L4 Port号码	333 (0 - 65535)
协议关键字	IGMP
协议号码	2 (1 - 255)

- **ACL ID -** 显示和指定 ACL 的 id。
- 端口**(s) -** 选择端口与此 ACL 相关联。
- 方向 - 此栏定义在此接口 ACL 过滤方向。
- 规则 - 显示和指定 ACL 相关的规则编号.
- 动作 - 此栏显示每一规则相关联的动作。可能的值是 Deny 或 Permit。
- 符合每项 - 指定一符合条件，此条件中所有数据包都符合 ACL 及规则号码所定义的 ACL 规则。其值为 False 或 True。当此值设为 True 时，（，）下面栏将无法输入
- 源 IP 地址 - 指定源 IP 地址给此规则
- 来源 IP 掩码 - 指定来源 IP 掩码给此规则.
- 目的地 IP 地址 - 指定目的地 IP 地址给此规则
- 目的地 IP 掩码 - 指定目的地 IP 掩码给此规则.
- 来源 L4 Port 关键字 - 指定符合条件的源第四层端口类别给此规则.
- 来源 L4 Port 号码 - 符合条件的源第四层端口号给此规则. 其值为 0 到 65535.
- 目的地 L4 Port 关键字 - 指定符合条件的目的地第四层端口类型给此规则.
- 目的地 L4 Port 号码 -指定符合条件的目的地第四端口层端口号给此规则. 其值为 0 到 65535.
- 协议关键字 - 指定规则过滤哪种协议, 可能的值为 IGMP, ICMP, IP, TCP, UDP.
- 协议号码 - 指定与此 ACL 关联的协议号码

- **服务类型** -给此规则指定服务类型，为 IP DSCP, IP Precedence 或 IP TOS.每一服务类型有其相关参数须配置，如下:

  IP DSCP

  - **IP DSCP -** 此值是指定的, 如 0 到 63 之间的任意一个整数.

  IP Precedence

  - **IP Precedence -** 优先值是一个 0 到 7 之间的整数.

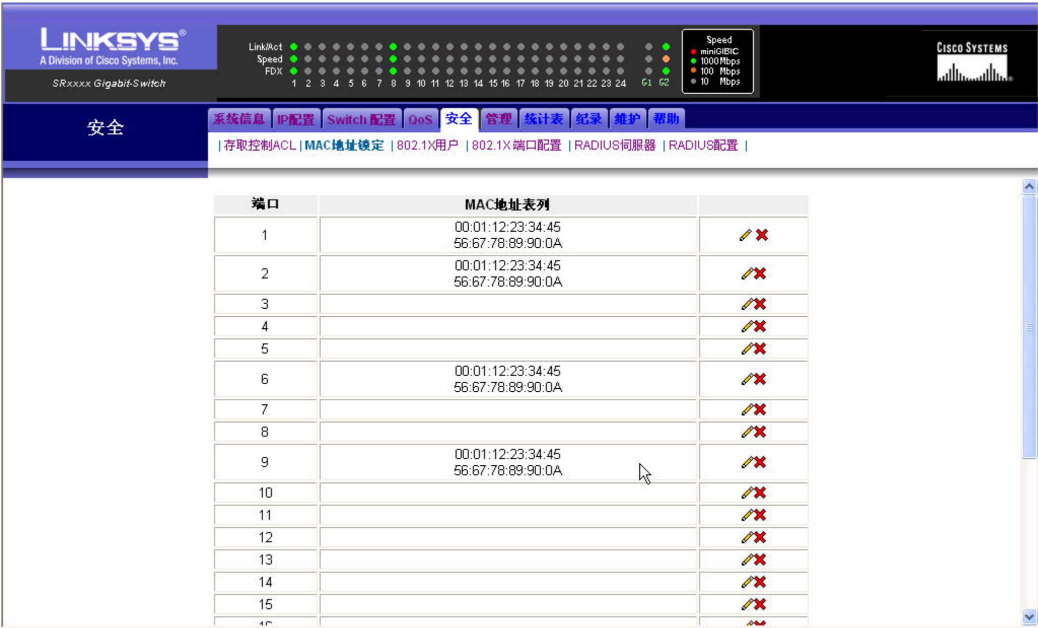
  IP TOS

  - **TOS Bits** - TOS Bits 的值是一个从 00 到 FF 的两位十六进制数.
  - **TOS 掩码-** TOS 掩码的值是一个从 00 到 FF 的两位十六进制数.

5.7.2 MAC 地址锁定

设置 MAC 地址锁定。指向菜单选项'安全'并点击'**MAC 地址锁定**'。将出现以下屏幕。

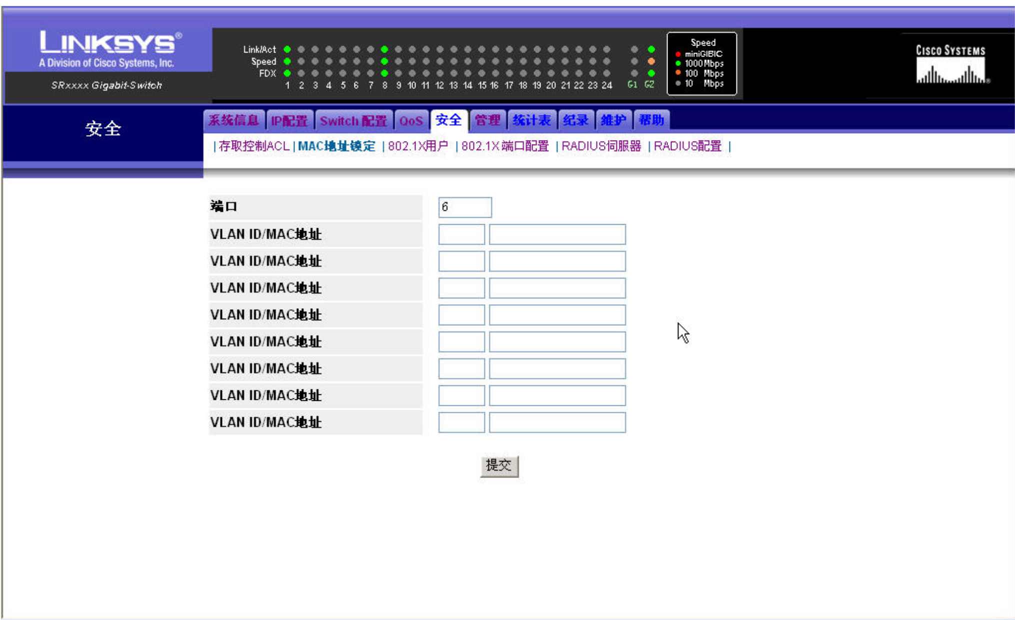
图 **5-59** MAC 地址锁定 屏幕



此表列出各端口所锁定的 MAC 地址. 点击端口图像' ✏ ' 以配置该端口将要锁定的 MAC 地址,或点击图像' ✖ ' 以清除端口所~~有~~锁定的 MAC 地址。

配置端口锁定的 MAC 地址，将出现以下屏幕。

图 **5-60** 端口 MAC 地址锁定配置屏幕



每一端口可锁定 8 个 MAC 地址. 必须输入此端口欲锁定的 MAC 地址在哪一 VLAN 及此 MAC 地

址.

5.7.3　802.1X 用户

设置 **802.1X** 用户参数。指向菜单选项'安全'并点击'**802.1X** 用户'。将显示出一个与下图相似的屏幕：

图 **5-61**　802.1X 用户屏幕



802.1X 用户表—显示所有用户登录信息。此中表包括下列信息

- 用户 - 显示于系统登录指定用户所属的登录表列.
- 表列名称 - 显示登录表列的表列名称.
- 端口 - 显示用户列表中指定用户所访问的指定端口.

启动 **802.1X**　– enable 或 disable 802.1X 模式.注意启动此模式会造成当前联机中断,必须重新联机才可管理此交换机.

此屏幕中的图标定义如下:

'✎'　– 修改 802.1X 用户所属登录表列与指定端口.

802.1X 用户配置

图 **5-62**　配置 802.1X 用户屏幕

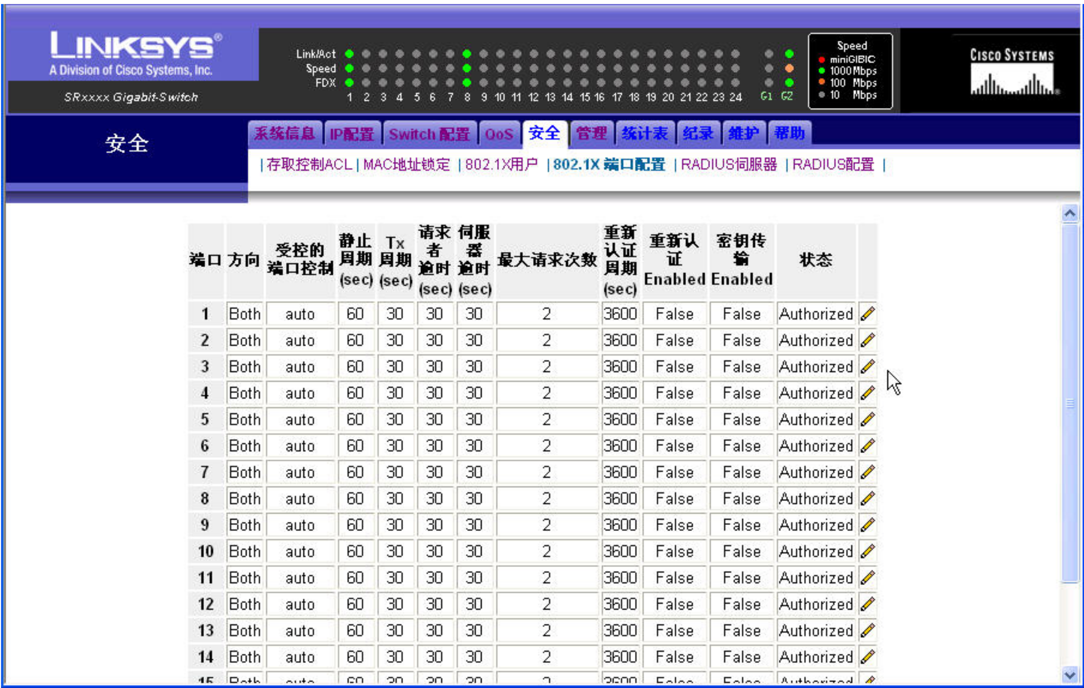
- **用户名** – 已配置的用户名,由章节 *5.8.1* **'用户帐号'**所定义的用户.
- **组别名称** - 已配置的登录表列. 由章节 *5.8.2* **'认证表列'**所定义的登录表列
- **端口** - 选择指定的端口.

如果用户被分配到一登录表列，而该表列要求远程认证，则对接口的所有访问经由 CLI 、互联网，和 telnet 会话将被阻拦直到认证完成。
注意为防止交换机被意外锁死,用户 admin 相关联的登录表列无法改变。

5.7.4 802.1X 端口配置

设置 **802.1X** 端口配置参数。指向菜单选项 **'安全'** 并点击**'802.1X 端口配置'**。将显示出一个与下面图示相似的屏幕.:

图 **5-63** 802.1X 端口配置屏幕



端口	方向	受控的端口控制	静止周期 (sec)	Tx 周期 (sec)	请求者逾时 (sec)	伺服器逾时 (sec)	最大请求次数	重新认证周期 (sec)	重新认证 Enabled	密钥传输 Enabled	状态
1	Both	auto	60	30	30	30	2	3600	False	False	Authorized
2	Both	auto	60	30	30	30	2	3600	False	False	Authorized
3	Both	auto	60	30	30	30	2	3600	False	False	Authorized
4	Both	auto	60	30	30	30	2	3600	False	False	Authorized
5	Both	auto	60	30	30	30	2	3600	False	False	Authorized
6	Both	auto	60	30	30	30	2	3600	False	False	Authorized
7	Both	auto	60	30	30	30	2	3600	False	False	Authorized
8	Both	auto	60	30	30	30	2	3600	False	False	Authorized
9	Both	auto	60	30	30	30	2	3600	False	False	Authorized
10	Both	auto	60	30	30	30	2	3600	False	False	Authorized
11	Both	auto	60	30	30	30	2	3600	False	False	Authorized
12	Both	auto	60	30	30	30	2	3600	False	False	Authorized
13	Both	auto	60	30	30	30	2	3600	False	False	Authorized
14	Both	auto	60	30	30	30	2	3600	False	False	Authorized

802.1X 端口配置表—此表中包括下列信息

- **端口** - 端口编号.
- **方向** - 指定端口的控制方向.此控制方向支配请求者与认证者之间进行协议交换的程度.这会影响是否使认证的可管理端口在两方向(disable 进入及出去的信息帧)或只在进入方向(只 disable 进入信息帧的接收).进行.
- **可管理端口控制** - 此端口运作的认证模式.其值可能是 ForceUnauthorized, ForceAuthorized, 或 Auto.
- **静止周期** - 在此端口认证者状态机器使用的定时器，用以定义时间周期,在周期内将不尝试去取得请求者. 此值以秒表示,其范围是 0 到 65535.
- **Tx 周期** - 在此端口认证者状态机器使用的定时器，用以决定何时去发送一 EAPOL EAP Request/Identity frame 给请求者. 此值以秒表示,其范围是 1 到 65535.
- **请求者逾时** - 在此端口认证者状态机器使用的定时器，用以对请求者记时. 此值以秒表示,其范围是 1 到 65535.
- **服务器逾时** - 在此端口认证者状态机器使用的定时器，用以对服务器记时. 此值以秒表示,其范围是 1 到 65535.
- **最大请求** - 在此端口认证者状态使用的最大次数，用以在逾时重新发送一 EAPOL EAP

Request/Identity frame 给请求者的次数. 其范围是 1 到 10.

- 重新认证周期- 在此端口认证者状态使用的定时器，用以决定何时对请求者重新认证.其值范围在 1 到 65535 之内.
- 重新认证 **Enabled** – 指示在指定端口重新认证是否 enable，其值可能是 True 或 False.
- 密钥传输 **Enabled** – 指示在指定端口是否传送密钥，其值可能是 True 或 False.
- **状态** –指示各端口的现况.

图标’’在此屏幕被用以配置一个期望的 802.1X 端口

配置 802.1X 端口

图 **5-64** 配置 802.1X 端口屏幕

端口存取实体	3
方向	Both
受控的端口控制	Auto
静止周期(secs)	60
传输周期(secs)	30
请求者逾时(secs)	30
伺服器逾时(secs)	30
最大请求次数	2
重新认证周期(secs)	3600
重新认证Enabled	False
密钥传输Enabled	False

提交

- **方向** —此栏用以对指定的端口配置控制方向。此控制方向支配请求者与认证者之间进行协议交换的程度.这会影响是否使认证的可管理端口在两个方向(disable 进入及出去的信息帧)或只在进入方向(只 disable 进入信息帧的接收)..
- **可管理端口控制**—此栏位用以设定指定端口的认证模式。控制模式可以是下列之一:

  forceunauthorized: 认证者port access entity (PAE)无条件地设定可管理端口为无认证.

  forceauthorized: 认证者port access entity (PAE)无条件地设定可管理端口为已认证.

  auto: 认证者port access entity (PAE)设定可管理端口模式为请求者,认证者,认证服务器之间进行协议交换的结果.

- **静止周期**—此栏设定此端口认证者状态使用的定时器的值,以秒计,用以定义时间周期,在周期内将不尝试去取得请求者。此静止周期就是一个周期,在此期间认证者在与

请求者之间交换失败时不再向请求者尝试去取得请求。静止周期的值必须在 0 到 65535 范围。

- **传输周期—**此栏设定此端口认证者状态使用的定时器的值，以秒计， 以决定何时发送一 EAPOL EAP Request/Identity frame 给请求者。传输周期的值必须在 1 到 65535 范围。
- **请求者逾时—**此栏设定此端口认证者状态使用的定时器的值，以秒计， 以对请求者计时。请求者逾时的值必须在 1 到 65535 范围。
- **服务器逾时—**此栏设定此端口认证者状态使用的定时器的值，以秒计， 以对认证服务器计时。服务器逾时的值必须在 1 到 65535 范围。
- **最大请求—**此栏设定此端口认证者状态在将请求者逾时之前重新发送 EAPOL EAP Request/Identity 最大次数。最大请求的值必须在 1 到 10 范围。
- **重新认证周期—**此栏设定此端口认证者状态使用的定时器的值，以秒计， 以决定何时作重新认证。重新认证周期的值必须在 1 到 65535 范围。
- **重新认证 Enabled—**此栏设定指定端口请求者的重新认证 enables 或 disable。重新认证的值必须是 **'True'** 或 **'False'** 。如果值是**'true'** 重新认证将发生。否则，重新认证不会被允许。
- **密钥传输 Enabled—**此栏设定指定端口请求者传送密钥 enable 或 disable。

5.7.5 RADIUS 服务器

设置 RADIUS 服务器。指向菜单选项’安全’并点击’**RADIUS 服务器**’。将显示出一个与下面图示相似的屏幕.:

图 **5-65** RADIUS 服务器屏幕



RADIUS 服务器表 —显示配置的 RADIUS 服务器。表包括

- **RADIUS 服务器 IP 地址** - 认证服务器的 IP 地址.
- **RADIUS Port** - 此服务器所使用的 port.
- **主要的服务器** - 服务器的类型. 其值有 Primary 或 Secondary

此屏幕中的图标被定义于下面:

’ ’ –创建 RADIUS 服务器

’ ’ –修改 RADIUS 服务器

’ ’ –删除 RADIUS 服务器

创建/修改 RADIUS 服务器

图 5-65　创建/修改 RADIUS 服务器屏幕

- **RADIUS 服务器 IP 地址—** 此栏设定 IP 地址用以连接到 RADIUS 服务器。每一 RADIUS 客户可设定 3 个服务器。
- **RADIUS Port —** 此栏设定UDP Port号码用以连接到RADIUS服务器。Port号码必须是在0和65535范围内。
- **秘密—**此栏位设定在RADIUS客户和RADIUS服务器之间共有的密钥。每一已设定的服务器都要有一被配置。密钥必须是由20个字母数字组成。此栏这里无法被显示，因为它已被加密。
- **主要的服务器 —** 此栏定义那一个已设定的服务器对此RADIUS客户来说是主服务器。此主服务器被用做处理RADIUS请求的缺省服务器。其它的服务器只有在主服务器无法到达时才使用。每一RADIUS客户最多可设定3个服务器。只有一个服务器为主服务器。
- **信息认证者—** 此栏用以将指定的RADIUS服务器的认证者属性enable或disable。信息认证者属性enable将对RADIUS客户和RADIUS服务器之间连接提供额外的安全。有些RADIUS服务器要求信息认证者属性enable才接受RADIUS客户的认证请求。
- **秘密已配置 —** 此栏指示秘密栏已被加密。

5.7.6 RADIUS 配置

设置 **RADIUS** 配置。指向菜单选项 **'安全'** 并点击 **'RADIUS 配置'**。将显示出一个与下图相似的屏幕.:

图 **5-66** RADIUS 配置屏幕

● **最大重新传送 —** 此栏设定当没有收到 RADIUS 服务器回应时重新发送请求数据包的最大次数。此值必须在 1 到 15 之间。

● **逾时持续时间 —**此栏设定逾时的值(以秒计), 如果没有收到回应的时间超过此值就必须重发请求给 RADIUS 服务器。逾时持续时间的值必须在 1 到 30 之间。

当配置最大重新传送和逾时持续时间时应考虑最大延迟时间。如果有多个 RADIUS 服务器被配置,在尝试下一个服务器之前每一个客户的最大重新传送的值将被用尽。重新传送除非超过所设定的逾时时间仍没有收到 RADIUS 服务器的回应。所以,由 RADIUS 应用收到回应的最大延迟等于所有服务器(重新传送次数乘以逾时持续时间)的总和。如果 RADIUS 请求由用户登录所产生, 所有用户接口将被阻拦直到 RADIUS 应用传回应答。

● **计帐模式—** 开启或关闭使 RADIUS 计帐功能。

配置 RADIUS 计帐服务器

只可设定一个 RADIUS 计帐服务器,使用 IP 地址及 UDP port 定义一计帐服务器.RADIUS 客户与RADIUS计帐服务器间有一共享的密钥. 点击图标' 🖹 '将显示出一个与下图相似的屏幕.

图 **5-66** RADIUS 配置屏幕

计帐伺服器IP地址	172.16.11.1
计帐伺服器Port	1813
秘密	
秘密已配置	No

提交

- 计帐服务器 **IP**地址 —计帐服务器使用的IP地址.
- 计帐服务器**Port** —计帐服务器使用的UDP port，范围0 - 65535.
- 秘密 —设置RADIUS服务器与RADIUS用户间的秘钥.

5.8 管理

指向指示灯面板之下的菜单选项, 点击标签 **'管理'**, 将出现以下屏幕.

图 **5-67** 管理屏幕



菜单包括以下参数:

用户帐号--让你配置用户帐号。参见章节 *5.8.1* '用户帐号'。

认证表列--让你配置认证表列。参见章节 *5.8.2* ' 认证表列'。

用户登录配置--让你配置用户登录配置。参见章节 *5.8.3* ' 用户登录配置'。

SNMP Community 配置--让你配置 SNMP Community。参见章节 *5.8.4* 'SNMP Community 配置' 。

Trap 接收--让你配置 SNMP Trap 接收器。参见章节 *5.8.5* '**Trap** 接收'。

Trap 标记--让你配置 Trap 标记。参见章节 *5.8.6* ' **Trap** 标记'。

5.8.1 用户帐号

设置用户帐号。指向菜单选项’**管理**’并点击’**用户帐号**’。屏幕将出现如图 5-67 的画面。

- **用户帐号表 —** 显示已配置的用户名称和他们的设置。此屏幕只有权限为readwrite的用户可看见。此表中包括下列信息
    - **用户名称** – 列出利用串口,Telnet 或者 WEB 来登录的以设定的用户.工厂的缺省值有二个用户名,admin 和 guest.
    - **存取模式** - 显示此操作者是否能够改变交换机的参数(Read/Write)或者只有阅览交换机的参数(Read Only). 工厂缺省设定 admin 有 Read/Write 存取权和 guest 有 Read Only 存取权.只有一个用户有 Read/Write 权限,可多达 5 个 Read Only 用户.
    - **SNMP v3 存取模式-** 指出 SNMP v3 访问权限给指定的登录用户.
    - **认证协议-** 指出指定的登录用户所使用的认证协议.有效的协议有 none, md5 或 sha.如果 md5 或 sha 被指定,此用户的登录密码将被用来作为 SNMP v3 的验证密码.
    - **加密协议** - 指出指定登录用户所使用的加密协议和密钥.有效的加密协议有 none 或 des.
    - **加密密钥** - 如果 DES 协议被指定,它将需要一个密钥,此密钥有 16 个字符长.如果 NONE 协议被指定，不需要提供密钥的.

此屏幕中的图标被定义于下面:

’ ’ ---创建一名新用户

’ ’ ---修改用户

’ ’ ---删除用户

创建/修改用户

图 **5-68**　配置用户帐号屏幕

- 用户名称 — 此栏用以指定一名新用户给此交换机。用户名称是 8 个字符和无大小写区分。工厂缺省用户为 admin 和 guest。
- 密码 — 此栏用以指定用户密码。此密码由八个字母数字组成。名称和密码不区分大小写。
- 确认密码 — 重新输入密码以确认它正确地被输入。
- 存取模式 — 此栏~~位~~用以指定操作员是否能改变交换机的参数 (Read/Write) 或只能查看参数(Read Only) 。作为工厂缺省,admin 有 Read/Write 权和 guest 有 Read Only 权。只有一个用户有 Read/Write 权限,可多达 5 个 Read Only 用户。
- **SNMP v3** 存取模式 — 此栏位定义 SNMP v3 访问权限给指定的登录用户。有效的访问模式为 **readonly** 或 **readwrite**。
- 认证协议 — 此栏定义指定的登录用户所使用的认证协议.有效的协议有 none, md5 or sha.如果 md5 或 sha 被指定,此用户的登录密码将被用来作为 SNMP v3 的论证密码。
- 加密协议 —此栏定义指定登录用户所使用的加密协议和密钥。有效的加密协议有 none 或 des。
- 密钥 — 如果加密协议是 des, 它将需要一个密钥, 此栏用以定义密钥。此密钥有 16 个字符长.如果 NONE 协议被指定,不需要提供密钥的。

5.8.2 认证表列

设置认证表列。指向菜单选项'**管理**'并点击' **认证表列**'。 将出现以下屏幕。

图 **5-69** 认证表列屏幕



认证列表用以配置不同的认证方式,如下图所示,认证方法有三种, local,radius,reject.

图 **5-70** 认证配置屏幕



5.8.3 用户登录配置

设置用户登录配置。指向菜单选项**'管理'**并点击**'用户登录配置'**。 将出现以下屏幕。

图 **5-71** 用户登录配置屏幕



将用户配置到所定义的认证表列中,如下图所示.

图 **5-72** 用户登录配置屏幕



5.8.4 SNMP Community 配置

设置 SNMP Community。指向菜单选项**'管理'**并点击**'SNMP Community 配置'**。将出现以下屏幕。

图 **5-73** SNMP Community 配置屏幕



SNMP Community 表 —此表中显示配置的 SNMP community 信息。信息中包括下列项

- **SNMP Community 名称** - 显示 SNMP Community 的名称.
- **客户 IP 地址** - 一个在该地址的设备将接受带相关 community 的 SNMP 数据包.
- **客户 IP 掩码** - 一个掩码，用以与请求实体的 IP 地址与指定 IP 相比较之前做与运算在.
- **存取模式** – 给此 community 的访问权限.
- **状态** - 此 community 访问实体的状态.

此屏幕中的图象定义如下：

' 🗎 ' –创建新 community

' ✎ ' –修改 community

' ✖ ' –删除community

创建/修改 Community

图 **5-74** 创建/修改 Community 屏幕

SNMP Community名称	public
客户IP地址	0.0.0.0
客户IP掩码	0.0.0.0
存取模式	Read Only
状态	Enable

提交

- **SNMP Community 名称** - 此栏用以定义 SNMP Community 的名称。是一个有大小写区分的 16 个字母数字组成。
- **客户 IP 地址**-此栏用以定义 IP 地址。此 IP 地址在该处的设备将接受带相关 community 的 SNMP 数据包。.缺省值是 0.0.0.0 。
- **客户 IP 掩码** - 此栏用以定义 IP 掩码。此掩码用以将请求实体的 IP 地址在与指定 IP 相比较之前做与运算。.缺省值是 0.0.0.0。
- **存取模式** - 此栏定义 community 字符串的访问权限。可由下拉菜单选择 Read/Write 或 Read Only。
- **状态** -如果一 SNMP Community 被 enable,一个与此 community 相关连的 SNMP 管制器就可根据它的访问权限管理此交换机。如果 Community 被 disable,使用此 Community 的 SNMP 要求就不会被接受。在这状况下与此 community 相关连的 SNMP 管制器就无法管理此交换机直到 enable 状态被改回。

5.8.5 Trap 接收

设置 Trap 接收器。指向菜单选项**'管理'**并点击**'Trap 接收'**。将出现以下屏幕。

图 **5-75** Trap 接收屏幕



Trap 接收表 — 显示 SNMP trap 接收。Trap 信息被寄发横跨网络到 SNMP 网络管理员。这些信息警告管理员发生在交换机之内或在网络的事件。同时支持六个 trap 接收。此表中包括下列信息

- **SNMP Community 名称** – SNMP trap 数据包的 Community 字符串被传送给 Trap 管理员。此名称由最长 16 个字母数字组成，有大小写区分。
- **IP Address** -拥有此 ip 地址的备将接收 SNMP Trap.
- **Status** –显示 Trap 接收状态(enable 或 disable).

此屏幕中的图标定义如下:

' ' –创造建 trap 接收者

' ' –修改 trap 接收者

' ' –删除 trap 接收者 r

创建/修改 Trap 接收者

图 **5-76** 创建/修改 Trap 接收屏幕

- **SNMP Community 名称** — SNMP Trap 名称。名称的最大长度是 16 个区分大小写的字母或数字字符。
- 客户 **IP** 地址 — 此栏用以指定 IP 地址。在该 ip 地址的设备将接收 SNMP trap。
- 状态 — 激活或撤销 SNMP trap。“enable”表明能接收 trap。“disable”表明不能接收 trap。

5.8.6 Trap 标记

设置 Trap 标记。指向菜单选项**'管理'**并点击**'Trap 标记'**。将出现以下屏幕。

图 5-77



- **认证 Trap -** 此栏定义是否发送认证 Trap。在下拉菜单中选择 enabled 或者 disabled。工厂缺省值是 disabled。
- **Link Up/Down -** 此栏定义是否发送链接通/断 Trap。在下拉菜单中选择 enabled 或者 disabled。工厂缺省值是 disabled。
- 多重用户 - 此栏定义是否发送多用户 Trap。在下拉菜单中选择 enabled 或者 disabled。工厂缺省值是 disabled。
- 广播风暴标记 - 此栏定义是否发送认证 Trap。在下拉菜单中选择 enabled 或者 disabled。工厂缺省值是 disabled。

5.9 统计

指向指示灯面板之下的菜单选项, 点击标签 **'统计'**, 将出现以下屏幕.

图 5-78



菜单包括以下统计信息:

交换机详细 －显示所有 CPU 流量的详细统计~~为~~。参见章节 5.9.1 '交换机详细'

交换机摘要 －显示所有 CPU 流量的总结。参见章节 5.9.2 '交换机摘要'

端口详细 －显示一个具体端口的详细统计。参见章节 5.9.3 '端口详细'

端口摘要 －显示一个具体端口的统计总结。参见章节 5.9.4 '端口摘要'

LA 摘要 －显示一个具体 LA 端口的统计总结。参见章节 5.9.5 'LA 摘要'

5.9.1 交换机详细

设置交换机详细。指向菜单选项 **'统计'** 并点击**'交换机详细'**。将出现以下屏幕。

图 5-79



- **Octets Received –** 此处理器(不含信息帧划分位,但含 FCS 八位字节)接收的八位字节数据总数.
- **Unicast Packets Received –** 交付给上一层协议的单播报总数.
- **Multicast Packets Received –** 接收的多播报的总数. 注意这些数不包括广播地址.
- **Broadcast Packets Received –** 接收到的广播报文总数. 注意不包括多播报.
- **Receive Packets Discarded –** 被选定丢弃的入站包数目, 该报文即使没有错误但仍被丢弃. 一个可能的原因是丢弃一个包以释放缓存空间.
- **Octets Transmitted –** 往接口外传送的八位字节总数, 含信息帧划分字符.
- **Packets Transmitted Without Errors –** 往接口外传送的报文总数.
- **Unicast Packets Transmitted –** 上一层协议要求发送给单播地址的报的总数, 包括丢弃或者不能发送的.
- **Multicast Packets Transmitted –** 上一层协议要求发送给多播地址的报的总数, 包括丢弃或者不能发送的.
- **Broadcast Packets Transmitted –** 上一层协议要求发送给广播地址的报的总数, 包括丢弃或者不能发送的.
- **Transmit Packets Discarded –** 被选定丢弃的出站报文数目, 该包即使没有错误但仍被丢弃. 一个可能的原因是丢弃一个以释放缓存空间.

- **Most Address Entries Ever Used –** 从最近一次重启后此交换机已学习的MAC 地址的最大数.
- **Address Entries in Use –** 此交换机的转发数据库地址表中已学习的和静态的条目数.
- **Maximum VLAN Entries –** 此交换机最多允许的的虚拟 ~~LANs~~ （局域网）(VLAN~~s~~)数目.
- **Most VLAN Entries Ever Used –** 自从最后一次重启以后在此交换机上的VLAN 的最大的数目.
- **Static VLAN Entries –** 目前在交换机上静态产生的 VLAN 的数目.
- **Dynamic VLAN Entries –** 目前在交换机上由 GVRP 注册产生的 VLAN 的数目.
- **VLAN Deletes –** 自从最后重启以后在此交换机上产生后又删除的 VLAN 数目.
- **Time Since Counters Last Cleared –** 此交换机的统计被清除之后经过的时间, 以日,时,分和秒计.

5.9.2 交换机摘要

设置交换机摘要。指向菜单选项 **'统计'** 并点击**'交换机摘要'**。将出现以下屏幕。

图 5-80



- **Packets Received Without Error –** 此处理器接收的无差错报文总数(包括广播报文和多播报).
- **Broadcast Packets Received –**接收到的广播包的总数.注意不包括多播报文.
- **Packets Received With Error –**收到的错误数据报.
- **Packets Transmitted Without Errors –** 由此界面外面向外传送无差错报文）总数
- **Broadcast Packets Transmitted –** 上一层协议要求以广播方式发送的报文总数,包括丢弃或者不能发送的.
- **Transmit Packet Errors –** 因为错误而不能传输的出站报文总数
- **Address Entries Currently in Use –** 此交换机的转发数据库地址表中已学习的和静态的条目数.
- **VLAN Entries Currently in Use –** 在目前 VLAN 表中的 VLAN 的数目.
- **Time Since Counters Last Cleared –** 此交换机的统计被清除之后经过的时间,以日,时,分和秒计.

5.9.3 端口详细

设置端口详细。指向菜单选项 **'统计'** 并点击**'端口详细'**。将出现以下屏幕。

图 5-81



此页将显示所选择的端口统计信息,如下:

- **ifIndex –** 此对象显示目前所选的界面.
- **Packets RX and TX 64 Octets –** 那些长度是 64 的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的 (包括坏的)接收和传送总数.
- **Packets RX and TX 65-127 Octets –** 那些长度在 65-127 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的 (包括坏的)接收和传送总数.
- **Packets RX and TX 128-255 Octets –** 那些长度在 65-127 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的 (包括坏的)接收和传送总数.
- **Packets RX and TX 256-511 Octets –** 那些长度在 265-511 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的 (包括坏的)接收和传送总数.
- **Packets RX and TX 512-1023 Octets –** 那些长度在 512-1023 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的(包括坏的)接收和传送总数.
- **Packets RX and TX 1024-1518 Octets –** 那些长度在 1024-1518 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的(包括坏的)接收和传送总数.
- **Packets RX and TX 1519-1522 Octets –** 那些长度在 1519-127 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的 (包括坏的)接收和传送总数.
- **Packets RX and TX 1523-2047 Octets –** 那些长度在 1523-2047 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的 (包括坏的)接收和传送总数.

- **Packets RX and TX 2048-4095 Octets** – 那些长度在 2048-4095 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的 (包括坏的)接收和传送总数.
- **Packets RX and TX 4096-9216 Octets** – 那些长度在 4096-9216 之间的八位字节(不含信息帧划分位,但含 FCS 八位字节)报的 (包括坏的)接收和传送总数.
- **Octets Received** – 在网络上接收的八位字节数据总数(包括坏的报文)(不含信息帧划分位,但含 FCS 八位字节). 此对象能够用以合理的评估以太网使用量.如果想得到的最大的精确度, etherStatsPkts 和 etherStatsOctets 对象应在共同时段之前和之后取样.这个方程的结果是这个使用量的值为以太网区段使用量百分比以百分之 0 到 100 计算.
- **Packets Received > 1522 Octets** – 那些比 1522 还长的八位字节(不含信息帧划分位,但含 FCS 八位字节)和其它适当的构成的报的(包括坏的)接收总数
- **Total Packets Received Without Errors** –接收的没有错误报文的总数
- **Unicast Packets Received** – 交付给上一层协议的单播报总数.
- **Multicast Packets Received** –接收到的多播报的总数.注意这些数不包广播地址的报.
- **Broadcast Packets Received** – 接收到的广播报总数.注意不包括多播报.
- **Total Packets Received with MAC Errors** –接收到的有 MAC 地址错误的包的总数.
- **Jabbers Received** – 那些长度超过 1518 的八位字节(不含信息帧划分位,但含 FCS 八位字节)和有任一的一个坏的结构检查顺序(FCS)与一个八位字节整数或者一个坏的 FCS 与一个八位字节非整数的分封接收总数.注意这些空闲定义与在 IEEE-802.3 8.2.1.5 部份(10BASE5)和 10.3.1.4 (10BASE2)部份里面的定义是不同的.这些文件定义空闲是以任何分封超过 20ms 为条件的.去侦测空闲的允许范围是在 20ms 到 150ms 之间.
- **Fragments/Undersize Received** – 在长度上小于 64 的八位字节(不含信息帧划分位,但含 FCS 八位字节)的报的接收总数.
- **Alignment Errors** – 长度在 64 和 1518 八位字节之间,包括 64 和 1518,但有一个坏的帧检验序列(FCS)与一个八位字节非整数的报的接收总数.
- **Rx FCS Errors** – 在 64 和 1518 八位字节之间,包括 64 和 1518,但有一个坏的帧检验序列(FCS)与一个八位字节整数的报的接收总数.
- **Overruns** –信息帧的总数,当此端口流入分封过载,且不能维持流入.
- **Total Received Packets Not Forwarded** – 那些经转发过程丢弃(例如:过滤)的接收到的有效信息帧总数.
- **Local Traffic Frames** – 在转发过程中因为目地地址未定位于此端口而被丢弃的信息帧总数.
- **82.3x Pause Frames Received** – 在此接口中所收到的 MAC 控制信息帧，其中运算代码为 PAUSE 的信息帧总数.当此接口运行在半双工模式的时候此总数不会增加.
- **Unacceptable Frame Type** – 在此端口因为信息帧类型无法接收的帧数目.

- **VLAN Membership Mismatch** – 在此端口由于去进入过滤而丢弃的信息帧数目.
- **VLAN Viable Discards** – 在此端口当在寻找一个特殊 VLAN 或者如果 VLAN 没有配置好而丢弃的信息帧数目.
- **Multicast Tree Viable Discards** – 当在（一 VLAN）寻找多播树时发生该树正被修改而丢弃的信息帧数目.
- **Reserved Address Discards** – 因为送往一个 IEEE 802.1 保留的地址和系统不支持而丢弃的信息帧数目.
- **Broadcast Storm Recovery** – 当广播风暴恢复生效的时候送往 FF:FF:FF:FF:FF:FF 地址而丢弃的信息帧数目.
- **CFI Discards** – 因 CFI 位被设定和在 RIF 里面地址是非典型形式而丢弃的信息帧数目.
- **Upstream Threshold** – 因未提供缺乏单元描述符给该分封的优先水平而丢弃的信息帧数目.
- **Total Packets Transmitted (Octets)** – 在网络(不含信息帧划分位,但含 FCS 八位字节)上所收到 (包括坏的)的八位字节总数. 此对象能够用以合理的评估以太网使用量. 如果想得到的最大的精确度, etherStatsPkts 和 etherStatsOctets 对象应在共同时段之前和之后取样.
- **Maximum Frame Size 1518** –
- **Total Packets Transmitted Successfully** – 在此端口已经被成功转发到它的区段的信息帧数目.
- **Unicast Packets Transmitted** – 上一层协议要求以单播发送的数据报的总数,包括丢弃或者不能发送的.
- **Multicast Packets Transmitted** – 上一层协议要求以多播发送的数据报的总数,包括丢弃或者不能发送的.
- **Broadcast Packets Transmitted** – 上一层协议要求以广播发送的数据报的总数,包括丢弃或者不能发送的.
- **Total Transmit Errors** – 单一的, 多重的和过多的碰撞总数.
- **Tx FCS Errors** – 已经被传送的报文总数,其长度(不含信息帧划分位,但含 FCS 八位字节) 在 64 和 1518 八位字节之间, 但也含有坏的具有完整八位字节帧校验序列 (FCS).
- **Tx Oversized** – 超过最大允许信息帧呎寸的信息帧总数.这个计数器有一个在 10 Mb/s 时每秒 815 个数的最大增量.
- **Underrun Errors** – 因为传输 FIFO 缓存变得空而丢弃的信息帧总数.
- **Total Transmit Packets Discarded** – 单一的,多重的和过多的碰撞信息帧总数.
- **Single Collision Frames** – 在特殊接口成功传送信息帧总数。该传输被规定只可有一个碰撞.

- **Multiple Collision Frames** – 在特殊接口成功传送信息帧总数。该传输被规定可有多于一个碰撞.
- **Excessive Collision Frames** – 在特殊接口成功传送信息帧总数。该传输失败因为过多的碰撞.
- **Port Membership Discards** – 在此端口因转发过滤而遭丢弃的数信息帧数目.
- **VLAN Viable Discards** – 当在在此端口寻找一个特殊 VLAN 或者如果 VLAN 没有配置好而丢弃的信息帧数目.
- **STP BPDUs Received** –在生成树中接收 BPDU's 网桥协议数据单元的数目.
- **STP BPDUs Transmitted** –从生成树中传输的 BPDU's 网桥协议数据单元的数目.
- **RSTP BPDUs Received** – 已的快速生成树协议网桥协议数据单元.
- **RSTP BPDUs Transmitted** – 已转发的快速生成树协议网桥协议数据单元.
- **MSTP BPDUs Received** – 已接收的多重生成树协议网桥协议数据单元.
- **MSTP BPDUs Transmitted** – 已转发的多重生成树协议网桥协议数据单元.
- **82.3x Pause Frames Transmitted** – 在此接口中所收到的 MAC 控制信息帧（，）其中运算代码为 PAUSE 的信息帧总数.当此接口是运行在半双工模式的时候此总数不会增加.
- **GVRP PDUs Received** – 在 GARP 层中接收 GVRP PDU's 的数目.
- **GVRP PDUs Transmitted** – 从 GARP 层中转发的 GVRP PDU's 的数目.
- **GVRP Failed Registrations** – 尝试 GVRP 注册无法完成的次数.
- **GMRP PDUs Received** – 在 GARP 层中接收 GMRP PDU's 的数目.
- **GMRP PDUs Transmitted** – 从 GARP 层中转发的 GMRP PDU's 的数目.
- **GMRP Failed Registrations** – 尝试 GMRP 注册无法完成的次数.
- **Time Since Counters Last Cleared** – 此端口的统计被清除之后经过的时间,以日,时,分和秒计.

5.9.4 端口摘要

设置端口摘要。指向菜单选项 **'统计'** 并点击**'端口摘要'**。将出现以下屏幕。

图 5-82



此页将显示所选择的端口统计信息,如下:

- **ifIndex –** 此对象显示目前所选的界面.
- **Total Packets Received without Errors** -处理器接收的~~分封~~（无差错数据报）(包括广播~~分封~~和多播~~分封~~)总数.
- **Packets Received with Error** -入站分封数目包含错误预防它们从有传输能力到上一层协议.
- **Broadcast Packets Received** -接收到的广播数据报的总数. 注意这些不包括多点传送数据报.
- **Packets Transmitted without Errors** -由此接口向外传送数据报总数.
- **Transmit Packet Errors** -因为错误而不能传输的出站数据报总数.
- **Collision Frames** -在此以太网段上预计的最佳冲突总数.
- **Time Since Counters Last Cleared** -此端口的统计被清除之后经过的时间, 以日, 时, 分和秒计.

5.9.5 LA 摘要

设置 **LA** 摘要信息。指向菜单选项 **'统计'** 并点击 **LA 摘要**。将出现以下屏幕。

图 5-83

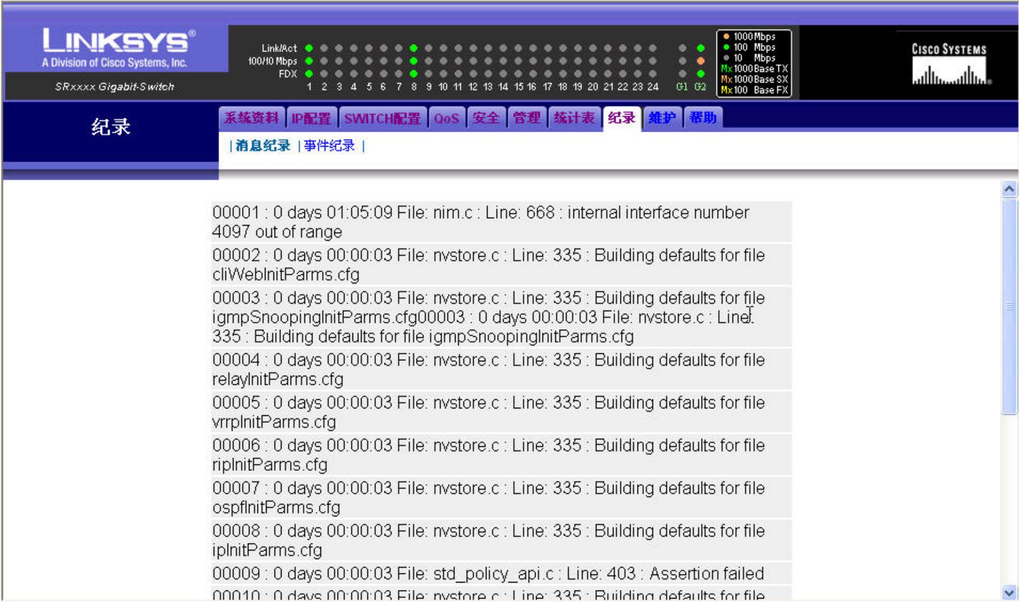


- **LACPDUs Received -** 在此聚合端口收到的被认为标准的有效的链路聚合控制 PDUs 数.
- **Marker PDUs Received -** 在此聚合端口收到的被认为标准的标记 PDUs 数.
- **Marker Response PDUs Received -** 在此聚合端口收到的被认为标准的标记响应 PDUs 数.
- **Unknown Packets Received -** 在此聚合端口收到的被认为未知结构数据.
- **Illegal Packets Received -** 在此集合端口被认为标准的有效连接集合 PDUs 数.
- **LACPDUs Transmitted -** 在此聚合口传输的有效连接聚合 PDUs 数.
- **Marker PDUs Transmitted -** 在此聚合端口传输的标记 PDUs 数.
- **Marker Response PDUs Transmitted -** 在此聚合端口传输的标记响应 PDUs 数.

5.10 纪录

指向指示灯面板之下的菜单选项, 点击标签 **'纪录'**, 将出现以下屏幕.

图 **5-84**



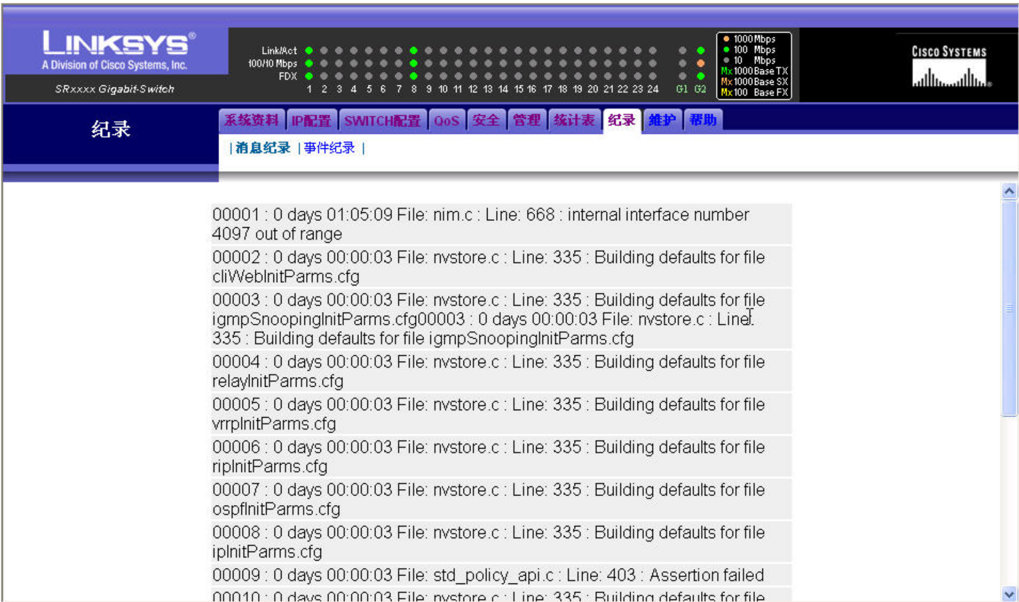
信息纪录 － 显示由交换机维护的信息纪录。参见 5.10.1 '信息纪录'。

事件纪录 － 显示包含错误信息的事件纪录。参见 5.10.2 '事件纪录'。

5.10.1 信息纪录

设置信息纪录。指向菜单选项**’纪录’**筛选和点击**’信息纪录’**。将出现以下屏幕。

图 5-85



显示由交换机维护的信息。此信息纪录包括系统追踪信息。

5.10.2 事件纪录

查看事件纪录。指向菜单选项’**纪录**’和点击’**事件纪录**’。将出现以下屏幕。

图 5-86



记入	文件名	线路	职务ID	信号	时间
00001: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00002: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00003: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00004: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00005: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00006: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00007: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00008: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00009: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00010: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00011: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00012: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00013: ERROR>	usmdb_si	1204	028D8250	00000003	0 0 3 42
00014: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0
00015: ERROR>	usmdb_si	1204	028D70B0	00000003	0 0 4 31
00016: EVENT>	bootos.c	276	03FFFE00	AAAAAAAA	0 0 0 0

- **Entry -**事件的编号.
- **Filename -** 事件起源的文件名称.
- **Line -** 事件的行数.
- **Task ID -** 事件的任务 ID.
- **Code -** 事件的编码.
- **Time -** 事件发生的时间.

5.11 维护

指向指示灯面板之下的菜单选项, 点击标签 **'维护'**, 将出现以下屏幕.

图 **5-87** 维护屏幕



菜单包括以下维护参数:

网络连通性—. 参见章节 *5.11.1* '网络连通性'.

Telnet —. 参见章节 *5.11.2* '*Telnet*'.

串口—. 参见章节 *5.11.3* '*Serial Port*'.

TFTP —. 参见章节 *5.11.4* '串口'.

重置—参见章节 *5.11.5* '重置'.

Ping —. 参见章节 *5.11.6* '*Ping*'.

5.11.1 网络连通性

设置网络连通性参数。指向菜单选项**'维护'**并点击**'网络连通性'**。将出现以下屏幕。

图 **5-88** Network Connectivity 屏幕

- 内建 **MAC地址** —显示给交换机烧录的MAC地址.
- 目前的网络配置协议—此栏显示目前使用的网络配置协议
- **HTTP Server** —定义交换机是否允许从web浏览器进行访问, Enabled意味着交换机是可从一个web浏览器进行管理的.工厂缺省值是enabled.
- **IP HTTP Secure** — 定义是否以 IP HTTP 安全模式来使用 web 浏览器进行访问. 工厂缺省值是 disabled.
- **IP HTTP Secure Protocol** — 定义使用 IP HTTP 安全模式所用的协议.
- **IP HTTP Secure Port** —定义使用 IP HTTP 安全模式所用的端口.

- 内建 **MAC地址** —显示给交换机烧录的MAC地址.
- 目前的网络配置协议—此栏显示目前使用的网络配置协议
- **HTTP Server** —定义交换机是否允许从web浏览器进行访问, Enabled意味着交换机是可从一个web浏览器进行管理的.工厂缺省值是enabled.
- **IP HTTP Secure** — 定义是否以 IP HTTP 安全模式来使用 web 浏览器进行访问. 工厂缺省值是 disabled.
- **IP HTTP Secure Protocol** — 定义使用 IP HTTP 安全模式所用的协议.
- **IP HTTP Secure Port** —定义使用 IP HTTP 安全模式所用的端口.

5.11.2 Telnet

设置 Telnet 参数。指向菜单选项**'维护'**并点击**'Telnet'**。将出现以下屏幕。

图 **5-89** Telnet 屏幕



- **闲置逾时** - 此栏~~位~~定义在注销一个 Telnet 对话之前可保持多少分钟不动作。如果为 0 表示将不会逾时,其值为 0 到 160 之间的某一个数。工厂缺省值是 5。
- **Telnet Sessions 的最大数量** - 此栏位定义最多可建立几个 Telnet 对话。如果为 0 表示将不可使用 Telnet 对话。工厂缺省值是 5。
- **准许新的 Telnet Sessions** - 此栏位定义是否可建立新的 Telnet 对话。工厂缺省值是 YES。

5.11.3 串口

设置串口参数。指向菜单选项**'维护'**并点击**'串口'**。将出现以下屏幕。

图 **5-90** 设置串口参数屏幕



- **串口登录逾时** - 此栏定义控制台保持多少分钟不动作的最大连接时间(分钟)。其值为 0 到 160 之间的某一个数。工厂缺省值是 5。
- **波特率(bps)** - 此栏定义终端机接口的通讯速率。这可以从下拉菜单中去选择. 其值有 1200, 2400,4800, 9600, 19200, 38400,57600,和 115200,工厂缺省值是 115200。
- **字符大小 (bits)** - 在一个字符中的位数, 此值永远是 8.
- **流量控制**- 无论硬件的流量控制是 enabled 或者是 disabled,它总是 disabled.
- **终止位** - 其停止位数始终是 1.
- **奇偶检测** - 此用在串口的奇偶检测方法,它总是一个 none.

5.11.4 TFTP

设置 TFTP 参数。指向菜单选项**'维护'**并点击**'TFTP'**。将出现以下屏幕。

图 **5-91** TFTP 屏幕



- **传输** - 此栏定义通过 TFTP 来接收/发送文件.其表示方法是下载给交换机和上传给服务器。
- **数据类型** - 此栏定义上传或下载的类型.其类型有配置文件,错误 Log,信息 Log 和 Trap Log。
- **档名** - 此栏定义上传或下载的文件名称。
- **服务器 IP 地址** - 此栏定义 TFTP 服务器的 IP 地址。

5.11.5 重置

设置重置命令。指向菜单选项'**维护**'并点击'**重置**'。将出现以下屏幕。

图 **5-92** Reset 屏幕



此屏幕显示三个按钮，其功能如下:

- **存储进快闪式存储器** – 将所有配置存到快闪储存器。所有配置改变会立即生效, 但未储存。必须存到快闪储存器，系统重新激活后配置仍有效。
- **复位成缺省值** - 此功能将所有配置参数复位成缺省值.
- **系统重启** - 重新激活交换机会造成此交换机的所有运作停止. 此会话将中断, 你必须在重新激活交换机后重新登录. 任何未储存的改变都将失去.

5.11.6 Ping

设置 Ping 命令指向菜单选项**'维护'**筛选和点击**'Ping'**。以下屏幕将出现。

图 **5-93** Ping 屏幕



- **IP Address -** 此栏位定义另一台计算机IP地址。
- **Ping —**此命令检查是否其它计算机是在网络上且可听到连接。使用此命令，配置交换机为网络(in-band) 连接。来源和目标设备必须有 Ping 程序 enable 和运行在 TCP/IP 上层。交换机可被由任一连在缺省 VLAN 的工作站 Ping 到，只要在交换机和工作站之间有一个实体的连接。终端机界面发送三个 Ping 到目的地工作站。